

Quantum Key Distribution and Blockchain

Securing the Future of Financial Transactions

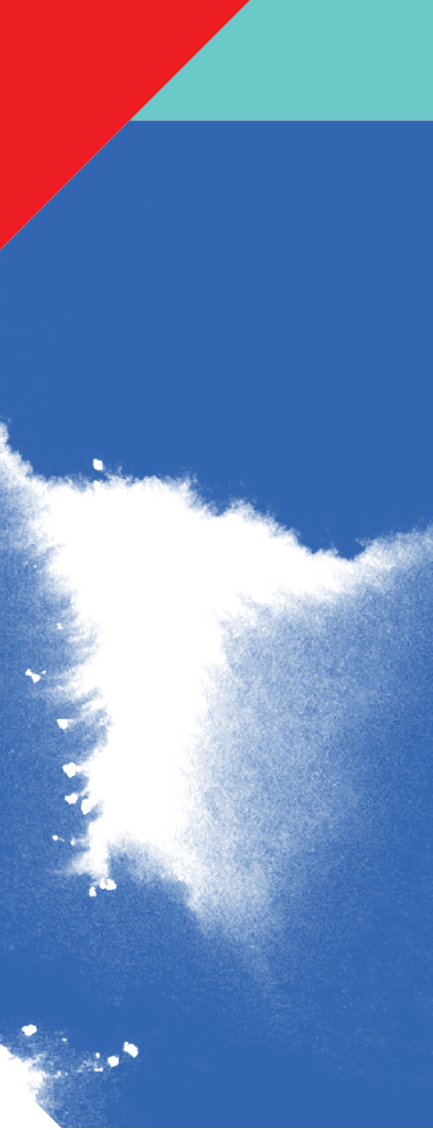
INTRODUCTION

While blockchain technology is arguably one of the most disruptive and innovative technologies to emerge in the last decade, there is another technology on the horizon that could undermine the security that blockchain promises: quantum computing. The power of quantum computing technology can challenge the security of any system that relies on certain mathematical algorithms for security, which blockchain currently does.¹

Sending data electronically between two sites makes it vulnerable to interception, and even public key encryption of the data in transit is vulnerable to a “harvest now and decrypt later” attack. This means that an attacker systematically records the encrypted data in transit, with the intent of decrypting it at their leisure when quantum computers become sufficiently powerful to break cryptography. This threat is becoming more urgent with the speed at which quantum computing is evolving, potentially making quantum computers capable of dramatically reducing the time to decrypt data protected with public key cryptography.

Quantum Key Distribution (QKD) technology takes advantage of the laws of quantum mechanics and allows two parties to agree on the same shared secret key and detect whether a third party is attempting to eavesdrop on their key agreement protocol. QKD is already capable of supporting mission-critical applications in metropolitan areas today, where applicable, alongside post-quantum cryptography in a hybrid approach. The use of QKD as part of a hybrid solution to quantum resistance can offer everlasting security, ensuring that a harvest and decrypt attack cannot succeed against the underlying public key encrypted data.

This paper will explore the evolution of these technologies, a real-world application research study with Toshiba, JPMorgan Chase and Ciena, and the future of QKD.



“The use of QKD as part of a hybrid solution to quantum resistance can offer everlasting security, ensuring that a harvest and decrypt attack cannot succeed against the underlying public key encrypted data.”



What Is Blockchain?

Blockchain is a **distributed, immutable and secure**² electronic database that stores information in blocks. Traditionally, data is stored in tables. However, as the name implies, blocks store data as long strings of randomly generated numbers and letters based on the numbers and letters from the previous block. Each block has a predetermined capacity, and information is stored linearly and chronologically, with unique hashcodes that record and timestamp changes. Once the block reaches capacity, it is closed and linked to previous blocks, thus forming the blockchain. Each block is added to the chain in chronological order, making it an excellent ledger for recording transactions.

The security of the blockchain is underpinned by two principles: integrity and consensus. Integrity ensures that one party cannot make transactions on another party's behalf. Every digital signature is prescribed to a unique private key known only to its owner and verified using the owner's public key, making forgeries impossible. Finally, consensus describes how new entries into a block are accepted and validated. This makes it impossible to "lie" on a blockchain record, as the network as a whole must validate and approve the change before it is added to a block. Without this universal approval (the "consensus"), changes will not be recorded, eliminating the potential for data to be maliciously tampered with.

Due to their level of security and fidelity, blockchains are especially useful in the financial industry. They enable institutions to exchange payment related information quickly and securely with the end goal of developing a more efficient means of transferring payment information through custom applications. Simplifying this process improves the speed and accuracy of inter-institution payments, reducing the potential for returned payments and decreasing payment processing times.

What Is Cryptography?

Cryptography is a means of **securing information and communications**³ using codes so that only intended audiences can have access to private data. Cryptographic techniques use algorithms to transform (or "encrypt") messages so that they become indecipherable by parties that are not authorized. In addition to identity, cryptography methods protect for authenticity and integrity. Authenticity is proving your identity and integrity is protecting the data from unauthorized changes.⁴ There are two types of encryption algorithms: symmetric-key (or single-key) and asymmetric-key (or public-key) encryption.

- **Symmetric key encryption**⁵ relies on just one key to encrypt and decrypt electronic information; two entities communicating via symmetric-key encryption must agree on the shared key.
- With **asymmetric-key encryption**,⁶ two distinct but mathematically connected keys, one public and one private, are generated for each entity. Both keys are known to the originator of the content. Any message that was encrypted using the public key can be decrypted using the corresponding private key, and vice versa. An entity's public key can be freely shared to give other parties the opportunity to encrypt contents that only the owner of the public and private key pair can decrypt. Digital signature is achieved by signing using private key by the owner and verified using public key by receiver.



“In a macro view, the exponentially increasing processing power of quantum computers puts the current digital communication and information landscape at risk.”

The benefits of using blockchain narrow down to five key uses⁷:

1. **Enhanced security:** The immutability of the blockchain helps to reduce instances of fraudulent activity. Its distributed nature makes it difficult to modify the data and ensures confidence in the distributed view of the data. Its anonymizing capabilities and controlled access points make it an excellent option for preserving data privacy when paired with end-to-end encryption.
2. **Greater transparency:** Thanks to the distributed nature of the blockchain data, transactions are identically recorded in multiple locations. All members of a network will always see the same data at the same time. The strict chronological recording enables members to view the entire history of a transaction, reducing the potential for fraud.
3. **Instant traceability:** The strong date and timekeeping on the blockchain creates an audit trail that can prove the provenance of an asset down to the second. This is especially important for industries where fraud is rampant or for consumer concerns about the origins of a product.
4. **Increased efficiency and speed:** Blockchain increases the efficiency and speed of manual paperwork. Documentation and transaction details are stored on the blockchain, eliminating the need to exchange paper or reconcile multiple ledgers.
5. **Automation:** Automation is a key aspect of this increased speed and efficiency, especially with the use of smart contracts. In these contracts, once predetermined requirements have been met, the next step in the transaction process is triggered. This reduces the need for human intervention and third-party verification.

Threats from New Technologies

Powerful, effective and widely available quantum computers are several years away from existence. However, this technology continues to pose challenges to cybersecurity in both the short and long-term. As mentioned above, one immediate concern is the prevalence of “**harvest now and decrypt later**” attacks.⁸ Information with a long shelf life today is especially vulnerable to this kind of attack from dedicated malefactors.

In a macro view, the exponentially increasing processing power of quantum computers puts the current digital communication and information landscape at risk. Once Quantum computers are sufficiently powerful, they will be able to break existing public-key cryptography standards, threatening digital systems.



Combating this threat will require the implementation of quantum-resistant encryption standards, such as QKD, on a global scale. Governments and critical institutions (including banks and IT companies) should be developing quantum security plans and fostering a quantum-ready workforce while these threats remain theoretical.

Current Encryption Levels

Public-key encryption is widely used for several applications on the web. This method of cryptography assures the confidentiality, integrity and authenticity of electronic communications. Common public-key encryption algorithms used today include **RSA, Diffie-Hellman and elliptic-curve cryptography**.⁹ The security of these algorithms is based on the assumption that certain mathematical problems—such as decomposing very large numbers into prime factors—are extremely difficult for computers to solve.

Such assumptions have held true for decades. However, the rise of quantum computers threatens the security of current cryptography systems. Quantum computers and the qubits that power them can perform multiple calculations at once, giving them the ability to compute any entity's private key from the corresponding public key, and consequently crack typical encryption methods in far less time than current computing allows. Large-scale, commercial quantum computers have yet to be made widely available, but it is necessary for enterprises to shore up their defenses now while the technology exists in its nascent stages. Two options companies have to this end are first to replace existing computational encryption methods (based on different assumptions) with new ones that are hopefully more secure than existing ones or, second, to do away with assumptions entirely and rely on QKD to secure the quantum future.

The QKD option is perhaps the most promising, as this method relies on the laws of physics as opposed to computational assumptions to secure communications between two entities. This form of **quantum cryptography**¹⁰ is based on the measurement and no-cloning principles of quantum mechanics, which establish that it is impossible to measure the state of a particle without changing the nature of the particle itself. With QKD systems, symmetric cryptographic keys are initially represented in the form of photons of light, which obey the measurement and no-cloning principles. This means that if a third party (an “eavesdropper”) tries to intercept a QKD-generated key, the photons themselves will change and the key will no longer be viable, alerting the intended parties of the interference. Without the ability to intercept the key, the eavesdropper will not be able to decrypt messages that are encrypted using the key, ensuring the confidentiality of the system.

The **National Institute of Standards and Technology (NIST)**¹¹ currently provides direction and guidance to organizations seeking to improve cybersecurity risk management via utilization of the NIST Cybersecurity Framework. Created in collaboration with industry and government, the framework consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.



QKD Key Generation Advantages

Keeping data secure is one of the greatest challenges posed by the rapid development of today's information technology. Increasing amounts of sensitive data are stored on remote, cloud-based servers, making secure access to this data a predominant concern. Securing **data transmission** relies on encryption of information sent over public networks. Sharing data securely using QKD has become an essential commercial consideration for business.

Financial institutions have some of the most demanding IT and data-security requirements. They need to ensure real-time availability of data for banking transactions and applications, and at the same time protect sensitive client and proprietary information. Additionally, they are subject to increasing levels of compliance and regulatory requirements.

These institutions need to be able to transfer data securely from their data processing and recovery centers to their campus networks for real-time trading and transactional-data exchange. The data is processed by core banking applications and video conferencing tools over wide area networks.

QKD is the first step toward removing public-key assumptions from blockchain applications. It is used to distribute the secret keys important for protecting highly sensitive data critical to many industries. It protects data confidentiality in the finance, defense, utilities and health sectors as well as the critical infrastructure that underpins our smart cities and smart energy grid.

The essence of QKD security relies on encoding each bit of the key upon a single photon (particle of light) transmitted, for example through an ordinary optical fiber. Any attempt to read or copy the photons alters their encoding, allowing the secrecy of each key to be tested and guaranteed. A single photon cannot be split into smaller particles and cannot be copied without altering the information that is encoded within it. The latter is prohibited by the **no-cloning theorem described above**. This enables the high level of security that QKD provides.

By adopting QKD, organizations can protect their communication infrastructure from today's vast array of cyber threats, as well as those of tomorrow. Already, hackers are using techniques like harvest and decrypt to store data today with the aim of decrypting it once they have the capability to do so through advances with supercomputers, the realization of a quantum computer or the discovery of new techniques for cryptanalysis. With QKD, any data requiring long-term protection is not only secure in today's IT landscape, but also future-proofed to remain protected in the impending quantum age.



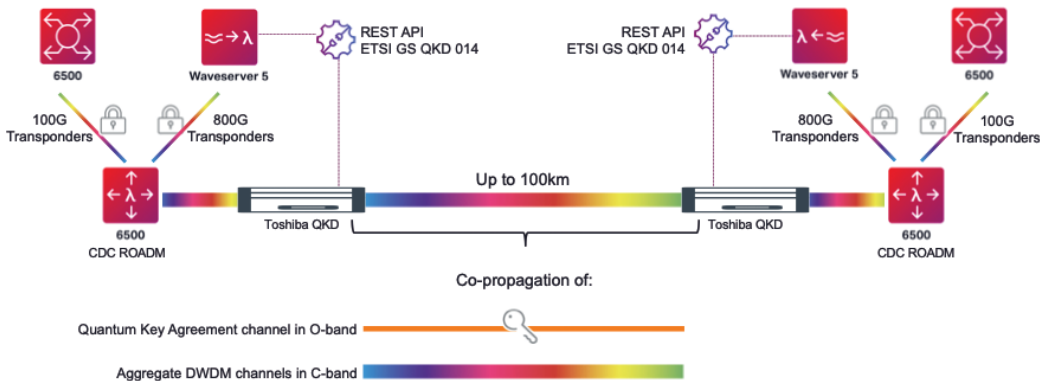
Real World Application: QKD Test Bed with JPMorgan Chase, Toshiba and Ciena

Toshiba worked with Ciena and JPMorgan Chase to conduct a joint experimental research study at JPMorgan Chase’s Optical Transport Lab in Columbus, Ohio and demonstrated the viability of a 800 Gbps quantum-resistant QKD-secured optical channel in mission-critical, metro-scale operational environments. This was a first for encryption in the industry, allowing the generation of QKD keys and the QKD-secured transmission of a very high volume of information on a single fiber. The test bed for this research study was carefully designed to mimic a real-world environment.

The research team demonstrated the ability of the newly developed QKD network to instantly detect and defend against eavesdroppers. It also studied the impact of realistic environmental factors on the quality of the quantum channel. The work also included the first demonstration of QKD securing a mission-critical blockchain application in the industry.

The findings of this research pave the way toward the deployment of quantum-secured optical channels based on QKD technology in high-capacity, metro-scale, mission-critical operational environments, such as Inter-Data Center Interconnects. The full research paper is available [here](#).

This schematic shows an example use case, with an AES encryptor obtaining keys from a Multiplexed QKD system to secure high-bandwidth data streams.





In the not-too-distant future, QKD will be a foundational technology for secure communications on the quantum internet.

Blockchain Advantage Using QKD

Permissioned blockchain networks often deal with large amounts of confidential information. While this information may be intended to be read by other parties in the network, it's critical that **data** confidentiality is retained while the data is in transit. Currently, the confidentiality of this data is protected through the use of standard public-key cryptographic schemes, which will not be sufficient against a quantum-capable eavesdropper in the future.

What's next?

Toshiba, and companies like JPMorgan Chase and Ciena, is at the forefront of developing technology for real-world applications. As the quantum computing era approaches, robust encryption will be of vital importance. Increasingly, QKD will be deployed in a similar capacity to how it has been demonstrated in the financial sector. In other areas, such as healthcare and national security.

Researchers envision applying QKD in similar ways to other contexts, in two main branches: first, through the technique of securing communication channels with QKD-secret keys for enhanced guarantees of confidentiality, as was done here; second, by replacing other instances of public-key cryptography with symmetric-key cryptography enabled by QKD, as in the case of integrity and consensus in the blockchain. The goal is to reduce the reliance on public-key assumptions whenever possible in order to reduce the potential attack surface exposed to quantum computers and future cryptanalysis.

In the not-too-distant future, QKD will be a foundational technology for secure communications on the quantum internet.

REFERENCES

1. “Quantum Computing Will Break the Blockchain and QKD Can Save It.” *Quantum Xchange*, <https://quantumxc.com/blog/quantum-computing-will-break-the-blockchain-and-qkd-can-save-it/>.
2. Hayes, Adam. “Blockchain Explained.” *Investopedia*, Investopedia, 15 Apr. 2022, <https://www.investopedia.com/terms/b/blockchain.asp>.
3. Richards, Kathleen. “What Is Cryptography?.” *SearchSecurity*, TechTarget, 27 Sept. 2021, <https://www.techtarget.com/searchsecurity/definition/cryptography>.
4. Saylor Academy. “Confidentiality, Integrity, and Authenticity: Attributes of secure communication” *Saylor Academy*, 5 May, 2022, <https://learn.saylor.org/mod/book/view.php?id=29682&chapterid=5263#:~:text=Cryptographic%20methods%20protect%20for%20confidentiality,the%20data%20from%20unauthorized%20changes>.
5. Smirnoff, Peter, and Dawn Turner. “Symmetric Key Encryption – Why, Where and How It’s Used in Banking.” *Cryptomathic*, <https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-howits-used-in-banking>.
6. Brush, Kate, et al. “What Is Asymmetric Cryptography?.” *SearchSecurity*, TechTarget, 27 Sept. 2021, <https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography>.
7. Pratt, Mary K. “Top 10 Benefits of Blockchain Technology for Business.” *SearchCIO*, TechTarget, 2 June 2021, <https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business>.
8. ISARA Corporation. “Protect against Harvest & Decrypt.” *ISARA Corporation*, <https://www.isara.com/solutions/use-cases/protect-against-harvest-decrypt.html>.
9. Lake, Josh. “What Is RSA Encryption and How Does It Work?” *Comparitech*, 22 Mar. 2021, <https://www.comparitech.com/blog/information-security/rsa-encryption/#:~:text=Under%20RSA%20encryption%2C%20messages%20are,known%20as%20the%20private%20key>.
10. “Quantum Encryption vs. Post-Quantum Cryptography.” *QuantumXC*, 22 Mar. 2022, <https://quantumxc.com/blog/quantum-encryption-vs-post-quantum-cryptography-infographic/>.
11. Nicole.keller@nist.gov. “Cybersecurity Framework: Getting Started.” *NIST*, 14 Apr. 2022, <https://www.nist.gov/cyberframework/getting-started>.

TOSHIBA

Toshiba America Inc.
Digital Solutions Division
5241 California Avenue
Suite 200, Irvine, CA 92617

Toshiba-Solutions@toshiba.com
Toshiba Global QKD Website