QuStream

2025

Quantum-Safe Encryption

www.qustream.com

The Future of Digital Security is at Risk

The world is rapidly transitioning into a fully digital economy, where blockchain transactions, financial systems, cloud storage, and even government infrastructures rely on encryption to secure sensitive data.

However, **current encryption standards will soon become obsolete**. Advances in quantum computing threaten to break RSA, ECC, and other classical cryptographic methods, making private keys, financial transactions, and enterprise security vulnerable to quantum-based attacks.

What happens when encryption fails?

How do businesses, financial institutions and Web3 projects prepare for a post-quantum world?

This is why **QuStream** was created

QuStream

As quantum computing becomes increasingly powerful, traditional encryption models face obsolescence, leaving the digital economy vulnerable. We bridge this gap by offering quantum-safe solutions that ensure simple transition and robust protection for all businesses, especially those operating in healthcare, banking and within the blockchain and cryptocurrency spaces.

504 bits quantum hardness

Mathematically proven cryptographic-hardness

Patent

The algorithm is currently patent-pending in the United States

Published

Cryptographically defined and published in Paper 2024/1145 on the ePrint Archive of the International Association for Cryptologic Research

Meet the Mind Behind QuStream

At the core of QuStream is Adrian Neal, an internationally recognized expert in Post-Quantum Cryptography, a two-time winner of the NATO Defence Innovation Challenge, and Senior Director & Global Lead for Post-Quantum Cryptography at Capgemini.

Adrian Neal
CEO QuStream

Over 40 years of cybersecurity career

Adrian has advised governments, defense agencies, financial institutions, and multinational corporations on sovereign/homomorphic encryption, post-quantum readiness, and global cybersecurity risk mitigation.

> He was the first cryptographic expert at UBS Warburg and the founder of Oxford BioChronometrics, developing cutting-edge fraud detection software cited by The Guardian, Financial Times, Wall Street Journal, and US Congress. He is an active member of the International Association for Cryptologic Research (IACR).

> With a Master's Degree in Software Engineering from Oxford University, Adrian has shaped encryption technologies for nearly four decades, and now, he is bringing a quantum-resistant encryption standard to the world.

Why Now? The Urgent Need for Quantum-Safe Encryption

With quantum computing advancing rapidly, traditional encryption methods like RSA and ECC are becoming obsolete. China's breakthrough in breaking RSA, along with massive investments from the US, EU, and China, is accelerating the timeline for real quantum threats.

2025

Majorana 1

Black Swan Event

The Majorana 1 breakthrough represents a major leap in quantum computing, advancing topological qubits with unprecedented stability. Unlike conventional superconducting qubits with error rates around 0.1%–1% per gate operation, Majorana-based qubits could achieve error rates as low as 10^{-4} due to their inherent topological protection. This drastically improves fault tolerance, paving the way for scalable quantum computers beyond 1,000 logical qubits.

Quantum computing is not decades away, **it is happening now**!

Who Needs Quantum-Safe Encryption?

Banks & Financial Institutions

Secure transactions, payment networks and digital banking against quantum threats

Governments & Defense Organizations

Protect classified data, communications, and infrastructure from cyber warfare

Cloud Storage & SaaS Providers

Encrypt customer data without reliance on vulnerable encryption

Insurance & Healthcare

Protect patient records, digital medical IDs and high-value claims data

Ecommerce & Retail

Encrypt customer transactions, payment data and loyalty programs

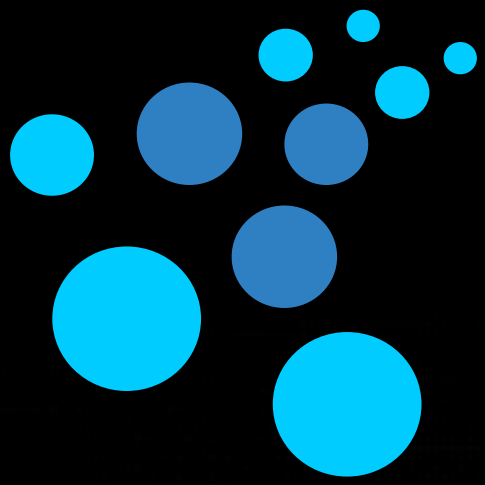
Blockchain Networks & Web3 Platforms

Ensure wallets, smart contracts and DeFi protocols remain quantum-resistant

Why QuStream?

QuStream is a fully decentralized, quantum-safe encryption solution that can be integrated into blockchains, financial institutions, enterprises and cloud-based security infrastructures.

Mathematically Proven Quantum Hardness	504 bit quantum hardness security, resistant to both classical and quantum attacks
Decentralized & Sharded Storage	Unlike centralized providers, we ensure that no single entity has full access to encryption keys
Enterprise-Grade Integration	Works with banks, governments, multinational corporations, blockchains and Web3 platforms
Transparent & Scalable Business Model	Clients pay only for the encryption they use, making it the most cost-efficient solution available



QuStream is not a concept, it is a fully developed, enterprise-ready encryption standard already being adopted by major institutions

www.qustream.com

contact@qustream.com