Every microsecond matters: *announcing the world's first NTS based on PQC from BeatQuantum.*

The world's first public network time service secured by post-quantum key exchange is now live in Coventry, United Kingdom, and is free to everyone.

Santosh Pandit · Founder, BeatQuantum · August 2026

The short version

- **Time is a security control, not plumbing.** Authentication, certificate validation, audit trails, replication and detection logic all assume the clock is right. When the clock is wrong, each of them fails quietly and at the same moment.
- **The protocol that sets the clock has been attacked for fifteen years.** Bitcoin timejacking and the timewarp attack in 2011, the NTP amplification floods of 2013 and 2014, the 2016 research on attacking NTP itself, and TETRA:BURST in 2023 all turned time synchronisation into an attack surface.
- **The modern fix is only half a fix.** Network Time Security authenticates time packets properly. Almost every public NTS server in service today performs its key exchange with classical cryptography, so recorded sessions can be decrypted once a cryptographically relevant quantum computer exists. That is a harvest now, decrypt later exposure sitting underneath the clock.
- **BeatQuantum has closed it.** Our Coventry server is the first NTS service in the world to run pure and hybrid post-quantum key exchange, with classical algorithms retained only to serve clients that have not yet upgraded. It is Stratum 2, sub-millisecond accurate, and free.

What breaks when the clock is wrong

A wrong clock does not announce itself. It presents as ten unrelated incidents at once, which is why time is usually the last thing an engineering team checks and the first thing an attacker moves. The failures group into four families.

Identity and trust stop working

- Tokens are rejected as expired or not yet valid, and Kerberos and single sign-on tickets fail.
- TLS handshakes fail because certificates read as not yet valid or expired.
- Signed requests stay acceptable for longer than intended, which opens the door to replay.

Distributed systems lose agreement

- Leader election and quorum health checks become unstable, and cluster state diverges.
- Database replication and change data capture apply or roll back changes on wrong timestamps.
- Cloud and Kubernetes control planes reconcile against times that no longer agree.

Evidence stops being evidence

- Logs arrive out of order, so incident timelines cannot be trusted or defended.
- Retention policies and regulated evidence ranges fall outside their required windows.

Detection misfires

- Intrusion detection correlation windows and SIEM rules run against skewed inputs, so real activity is missed and clean activity is flagged.

Where the damage lands first

Financial services is the obvious case, and it is not the only one. The sectors below share a common feature: a regulated or safety-critical process whose correctness is defined by an agreed time, not by a local opinion of it.

SECTOR	WHAT A MANIPULATED CLOCK DISRUPTS
Cloud and SaaS platforms	Authentication, metering and billing, distributed workflows, incident response
Cybersecurity operations	SIEM and SOAR correlation, detection logic, incident timelines
Energy and utilities	Grid operations, demand response, outage coordination
Financial services	Trading, banking core systems, payments, fraud detection
Government and public sector	Identity systems, records management, delivery of critical services
Healthcare	Health record access, clinical workflows, billing and coding, audit trails
Industrial control and manufacturing	SCADA, production scheduling, maintenance windows
Legal and compliance	Electronic discovery, regulated reporting, evidence integrity
Telecommunications	Billing, lawful event logging, network management
Transport and logistics	Fleet tracking, dispatch scheduling, shipment documentation

Sectors listed alphabetically. Exposure rises wherever the process is regulated, automated, or settled between two parties.

WHERE THE PROTOCOLS STAND TODAY

NTP, NTS, and the gap that remains

The Network Time Protocol carries time over UDP port 123 and offers close to no authentication in its classic form. Network Time Security is the modern extension. It performs a key exchange over TCP port 4460 and then delivers authenticated time packets over UDP port 123. Anyone relying on time should be running NTS.

NTS is a genuine improvement, and it leaves one problem open. Almost every server that offers NTS today performs that key exchange with classical algorithms. An adversary who can record the exchange keeps it. When a cryptographically relevant quantum computer becomes available, the recorded session keys can be recovered, the server can be impersonated, and false time can be injected into every client that trusted it. The exposure is created on the day the traffic is captured, not on the day the quantum computer arrives.

	CLASSIC NTP	NTS TODAY	BEATQUANTUM NTS
Time packets authenticated	No	Yes	Yes
Key exchange	None	Classical	Post-quantum, pure and hybrid
Resists harvest now, decrypt later	No	No	Yes
Serves clients not yet upgraded	Yes	Yes	Yes, classical retained for compatibility

THE ANNOUNCEMENT

The BeatQuantum time service

We have built and put into production the world's first network time server that runs the NTS extension with pure and with hybrid post-quantum algorithms. Selected classical algorithms are retained for backward compatibility and are used only where the client has not yet upgraded.

ATTRIBUTE	DETAIL
Host	beatquantum.com
Location	Coventry, United Kingdom
Classification	Stratum 2
Accuracy	Sub-millisecond
Key exchange	Pure post-quantum and hybrid post-quantum, classical retained for compatibility
Transport	Key exchange on TCP 4460, authenticated time on UDP 123
Availability	Production grade, offered free to everyone

How to treat it

The intended use is as an additional source in a pool you already run. It is a United Kingdom Stratum 2 server performing on a par with any production grade source, so it can be added alongside your existing servers without changing anything else. Doing so does not make the whole pool quantum resistant, and it is not meant to. It gives you three things at no cost and at no risk to your current arrangement.

- **Performance and stability evidence.** You observe how a post-quantum source behaves inside your own pool, over your own network, against your own existing sources.
- **A client compatibility test.** You find out immediately whether your clients negotiate post-quantum key exchange, and which ones fall back to classical.
- **A migration baseline.** The measurements you take now are the evidence you will need when you decide to move the whole quorum.

Users in the United Kingdom and Western Europe can treat it as suitable for production use on this basis. Users elsewhere may use it for research and experimental work, where the additional network distance is acceptable for the purpose.

How to connect

The service runs at `beatquantum.com`. Key exchange takes place over TCP port 4460. Time then flows as authenticated NTP over UDP port 123. Both ports must be open outbound. Any client supporting NTS will work, including chrony from version 4.0 and ntpsec.

For chrony, add the following line to `chrony.conf` and restart the service.

```
server beatquantum.com iburst nts
```

Verify with chronyc -N sources and chronyc authdata. The authentication mode should report NTS and the key establishment count should be non-zero.

Dedicated capacity

Government bodies, space agencies, exchanges, operators of critical national infrastructure and financial institutions that need capacity of their own should contact us. We will provide seven discrete NTS servers built to the specific requirement, for example sited at dealing room locations for high frequency trading.

Seven is a deliberate number. A time client does not trust a single source. It compares its sources and disciplines the clock to the majority it can agree with, discarding the ones that disagree. Four sources allow it to survive one server that is wrong or lying. Seven allow it to survive two and still hold a quorum.

That arithmetic is the reason a single post-quantum server is not a complete answer for an organisation with a hard requirement. If the remaining sources in the pool are classic NTP or NTS with classical key exchange, they form the majority, they decide the clock, and the harvest now, decrypt later exposure returns through them. A dedicated pool of seven puts the whole selection quorum on post-quantum key exchange.

BeatQuantum is the world leading centre of excellence in applied post-quantum cryptography.

> *Being second best is not an option.*

Santosh Pandit, Founder, BeatQuantum