الحوسبة الكمية وتهديدها لخوارزميات التشفير: نحو عالم ما بعد الكم

إعداد: أحمد البشير الصغير عمر- شبكة بلوكتشين ليبيا للأعمال (بالإستعانة بنموذج كلوود أوبس)

مقدمة: لماذا يجب أن نهتم بهذا وفي هذا الوقت؟

ما يجب أن يعلمه الجميع أن كل رسالة يتم إرسالها وكل تحويل مصرفي يتم وكل جواز سفر يتم إصداره محمي بنوع واحد من الرياضيات: التشفير بالمفتاح العام Public Key Cryptography. وهذا النوع من الرياضيات أصبح مهددا بأن يتم كسره يومًا ما أمام الحاسوب الكمي. والسؤال ليس «هل سيتم ذلك أم لا؟ بل متى؟».

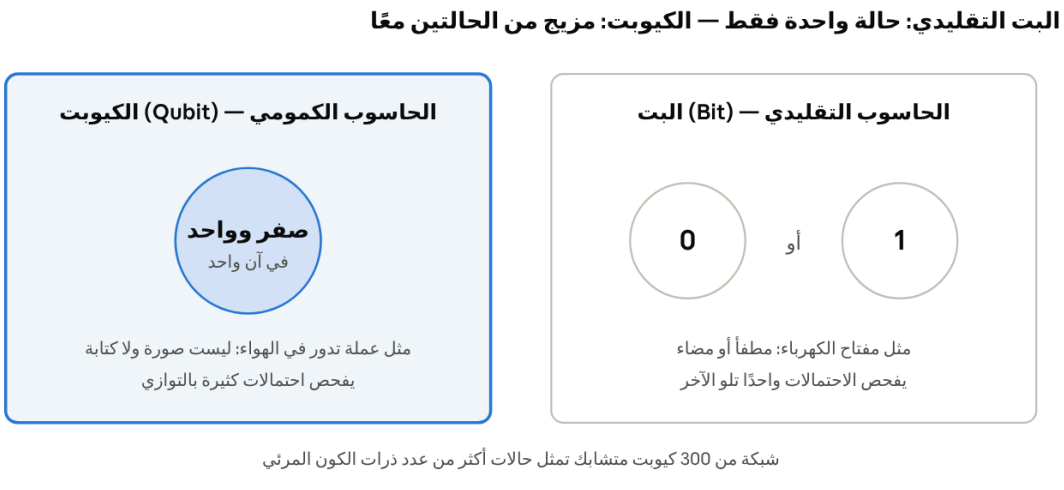
الحوسبة الكمومية ليست خيالًا علميًا. فشركات عملاقة مثل جوجل وآي بي إم تبني حواسيب كمية تتضاعف قدراتها عامًا بعد عام، والحكومات حول العالم وضعت بالفعل مواعيد نهائية للتخلي عن بروتوكولات التشفير الحالي. فالولايات المتحدة تستهدف إيقاف خوارزميات RSA وECC بحلول 2030 وحظرها نهائيًا بحلول 2035، والاتحاد الأوروبي أصدر خارطة طريق مماثلة.

الأخطر من ذلك أن التهديد قد بدأ فعليًا. ففي الوقت الحالي تتواجد عديد من الجهات التي تجمع اليوم بيانات مشفرة لفك تشفيرها لاحقًا عندما تنضج تقنيات الحواسيب الكمية عبر ما يعرف بهجوم «اجمع الآن، وفُكّ لاحقًا». وهذا خطر يهدد أي بيانات تحتاج سرية لأكثر من عقد: سجلات طبية، أسرار تجارية، مراسلات دبلوماسية، بيانات مالية، وهذا يجعلها معرضة منذ الآن رغم كونها الآن مشفرة ومحمية.

في هذا المقال حاولنا شرح المفاهيم بلغة بسيطة وتم التطرق إلى كيفية عمل الحوسبة الكمية، وكيف يعمل التشفير، ولماذا سيكسر الأول الثاني، وما أثر ذلك على البنوك والاتصالات والهويات الحكومية الرقمية والعملات المشفرة، وكيف حددت عديد الحكومات والمؤسسات خارطة الطريق لمحاولة تفادي هذا الخطر.

أولاً لنحاول أن نتعرف على كيف تعمل الحوسبة الكمية؟

الحاسوب العادي مبني ويفكر بوحدة تسمى «البت Bit»: وهي أصغر وحدة معلومات وتكون حالتها إما صفرًا أو واحدًا، مثل مفتاح كهرباء مطفأ أو مضاء. أما الحاسوب الكمي فيستخدم «الكيوبت Qubit»، وهو يستفيد من خصائص فيزياء الجسيمات دون الذرية ليكون في مزيج من الحالتين معًا — مثل عملة تدور في الهواء قبل أن تستقر.



الفرق بين البت التقليدي والكيوبت الكمومي

ثلاثة مفاهيم تكفي لفهم الصورة:

1. **التراكب (Superposition):** الكيوبت يكون في مزيج من الحالتين 0 و 1 في آن واحد، ما يسمح للحاسوب الكمي باستكشاف عدد هائل من الاحتمالات بالتوازي بدل من فحصها واحدًا تلو الآخر.
2. **التشابك (Entanglement):** كيوبتان متشابكان يرتبطان ببعضهما بحيث إن قياس أحدهما يحدد حالة الآخر فورًا، مهما بعدت المسافة بينهما. هذا ما يجعل قوة الحاسوب الكمي تنمو بشكل أُسي (مضاعف) مع كل كيوبت يضاف.
3. **القياس (Measurement):** عند قراءة النتيجة ينهار التراكب إلى إجابة واحدة. لذلك فالحاسوب الكمي ليس أسرع في كل شيء، بل فقط في مسائل محددة توجد لها خوارزميات كمية ذكية توجّه الاحتمالات نحو الإجابة الصحيحة.

المشكلة الهندسية الكبرى في عالم الحواسيب الكمية هي «الضجيج». فالكيوبتات هشة جدًا وتفقد حالتها بسرعة، لذا تحتاج آلاف الكيوبتات الفيزيائية لبناء «كيوبت منطقي» واحد مستقر عبر تصحيح الأخطاء الكمية. فكسر أحد بروتوكولات التشفير الحديث يتطلب آلاف الكيوبتات المنطقية (أي مئات الآلاف إلى ملايين الكيوبتات الفيزيائية) وهذا بالضبط ما تتسابق المختبرات لبنائه خلال العقد القادم إن لم يكن خلال السنوات القريبة القادمة.

السؤال المهم كم حاسوبًا كميًا نحتاج لكسر التشفير؟

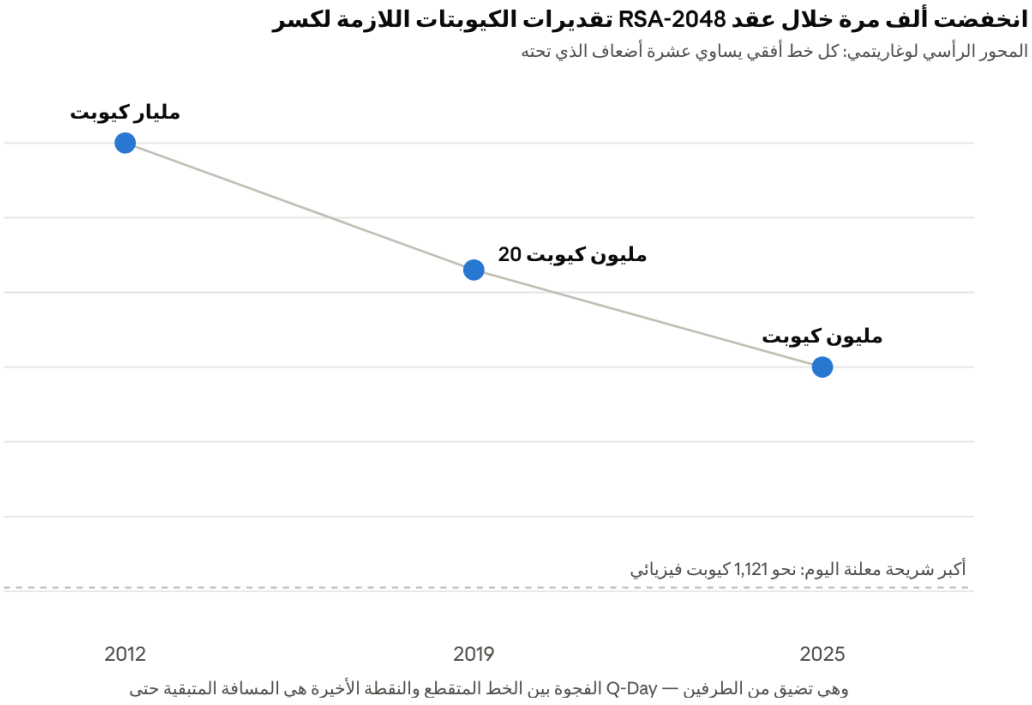
لفهم الفترة الزمنية المتبقية، لا بد من التفريق بين نوعين من الكيوبتات:

- **الكيوبت الفيزيائي:** الكيوبت الخام كما يُصنع في المختبر. وسنتخيله كشمعة في مهب الريح: يفقد حالته بسرعة بسبب أدنى اهتزاز أو حرارة أو إشعاع.
- **الكيوبت المنطقي:** كيوبت «موثوق» يُبنى من مئات أو آلاف الكيوبتات الفيزيائية التي تراقب بعضها وتصحح أخطاء بعضها، مثل حماية الشمعة بزجاج وحراس يعيدون إشعالها فور أي خفوت وهذا ما يسمى «تصحيح الأخطاء الكمي»، وهو العقبة الهندسية الكبرى.

والآن للتوضيح بشكل أكبر فإن كسر خوارزمية التشفير المهمة المعروفة ب RSA-2048 بإستخدام خوارزمية شور (خوارزمية كمية) فنحتاج إلى بضعة آلاف من الكيوبتات المنطقية المستقرة أو ما يعادل مئات الآلاف إلى ملايين الكيوبتات الفيزيائية. وحسب ما هو معلن عنه فإن أكبر الشرائح المعلنة عنها اليوم تحمل نحو ألف كيوبت فيزيائي فقط (شريحة IBM Condor بـ 1,121 كيوبت)، لكن المقلق ليس حجم الشرائح الحالية بل القلق ينشأ من اتجاهين يقتربان من بعضهما:

1. **المتطلبات تنخفض:** الخوارزميات تتحسن باستمرار. عام 2012 قُدر أن كسر RSA-2048 يحتاج نحو مليار كيوبت فيزيائي، وعام 2019 انخفض التقدير إلى 20 مليونًا (في زمن تشغيل حوالي 8 ساعات)، وفي 2025 نشر الباحث كريغ غيدني من غوغل تقديرًا بأقل من مليون كيوبت (في زمن تشغيل نحو أسبوع). ألف ضعف أقل في عقد واحد.
2. **الآلات تكبر وتتحسن:** شريحة Willow من غوغل (2024) أثبتت لأول مرة أن إضافة كيوبتات أكثر تقلل الأخطاء بدل أن تزيدها وهذا هو شرط التوسع الذي كان مفقودًا.

أما كسر منحنى secp256k1 المستخدم في شبكات العملات الرقمية بيتكوين وإيثريوم فتقدره ورقة Google Quantum AI (المنشورة في مارس 2026) بأقل من 500 ألف كيوبت فيزيائي ودقائق معدودة من التشغيل على المعماريات السريعة. أي أن مفاتيح العملات المشفرة (256 بت من نوع ECC) قد تسقط قبل مفاتيح RSA-2048 نفسها، وذلك لكون المسألة الحسابية لمفاتيح ECC أصغر حجمًا من منظور الخوارزمية الكمية.



ولكن كيف يعمل التشفير ولماذا هو عرضة للكسر من قبل الحواسيب الكمية؟

التشفير الحديث يقوم على فكرة بسيطة تستند على مسائل رياضية سهلة لتكوين البيانات المشفرة في اتجاه ومستحيلة عمليًا في الاتجاه المعاكس لكسر التشفير. كمثال عملية ضرب عددين أوليين ضخمين يستغرق جزءًا من الثانية، لكن تفكيك ناتج الضرب إلى عامليه الأوليين يستغرق من أقوى الحواسيب التقليدية مليارات السنين. على هذه الفرضية تم بناء أمن بيانات العالم الرقمي كله.

وللتوضيح أكثر فهناك نوعان رئيسيان من التشفير، والتمييز بينهما جوهري لفهم التهديد القادم من الحواسيب الكمية:

الخاصية	التشفير المتماثل (Symmetric)	التشفير غير المتماثل / بالمفتاح العام (Asymmetric)
الفكرة	مفتاح سري واحد للتشفير وفك التشفير	مفتاح عام منشور للتشفير، ومفتاح خاص سري لفكه
تشبيه	خزنة بمفتاح واحد يتشاركه الطرفان	صندوق بريد: أي أحد يضع رسالة، وصاحبه وحده يفتحه
أشهر الخوارزميات	AES، ChaCha20	RSA، ECC (ECDSA/ECDH)، Diffie-Hellman
الاستخدام	تشفير البيانات نفسها (ملفات، اتصالات)	تبادل المفاتيح، التوقيعات الرقمية، الهوية
المسألة الرياضية	خلط وتبديل معقد (لا بنية رياضية قابلة للاستغلال)	تفكيك الأعداد (RSA) أو اللوغاريتم المتقطع (ECC)
أثر الحاسوب الكمومي	يُضعف فقط (يعالج بمضاعفة طول المفتاح)	ينكسر بالكامل

في التطبيقات العملية التي نستخدم فيها عمليات التشفير فكلا النوعان يعملان معًا. عندما تفتح موقعًا آمنًا (وجود علامة HTTPS في المتصفح)، يُستخدم التشفير غير المتماثل أولًا للاتفاق سرًا على مفتاح مؤقت، ثم تُشفر بقية الجلسة بالتشفير المتماثل السريع. والتوقيعات الرقمية — التي تثبت أن الرسالة أو البرنامج أو المعاملة صادرة فعلًا ممن يدعي إصدارها — تعتمد كليًا على التشفير غير المتماثل. لذلك فإن نقطة الضعف الحقيقية أمام الحوسبة الكمية تتمثل في تقنيات التشفير غير المتماثل وهو للأسف الأساس الذي تقوم عليه الثقة في الإنترنت بكافة خدماته.

كيف ستكسر الحوسبة الكمومية التشفير؟

التهديد يأتي من خوارزميتين كميتين اكتُشفتا قبل أن توجد الحواسيب القادرة على تشغيلهما بعقود:

1. **خوارزمية شور (Shor, 1994):** وهي خوارزمية تحل مسألتي تفكيك الأعداد واللوغاريتم المتقطع بسرعة أُسية. بمعنى آخر فإن المسألة التي تستغرق مليارات السنين على حاسوب تقليدي تصبح مسألة ساعات أو أيام على حاسوب كمي كبير بما يكفي. هذه الخوارزمية لتكسر خوارزميات RSA وECC وDiffie-Hellman بالكامل وليس فقط إضعافًا لها.
2. **خوارزمية غروفر (Grover, 1996):** وهي خوارزمية تسرّع ما يعرف بالبحث الأعمى بشكل تربيعي فقط، فتخفض أمان التشفير المتماثل إلى النصف فعليًا. فمعيار AES-128 يصبح بقوة 64 بت (وهو غير آمن)، ولكن AES-256 يبقى بقوة 128 بت (وهو آمن). المعالجة في هذه الحالة أبسط وتستند لمضاعفة طول المفاتيح.

في الجدول التالي نحاول تلخيص مصير أهم الخوارزميات المستخدمة اليوم أمام الحوسبة الكمية:

الخوارزمية	النوع	أين تُستخدم	الخوارزمية الكمومية المهاجمة	المصير
RSA-2048	مفتاح عام	شهادات HTTPS، البريد، التوقيعات	شور	كسر كامل
ECC (ECDSA / ECDH)	مفتاح عام	العملات المشفرة، TLS، الجوازات، الهواتف	شور	كسر كامل
Diffie-Hellman	تبادل مفاتيح	VPN، الاتصالات الآمنة	شور	كسر كامل
AES-128	متماثل	تشفير البيانات	غروفر	ضعيف — يُستبدل بـ AES-256
AES-256	متماثل	تشفير البيانات الحساسة	غروفر	آمن
SHA-256 / SHA-3	دوال تجزئة	سلاسل الكتل، التواقيع، كلمات المرور	غروفر	آمن عمومًا (مع مخرجات طويلة)

والخلاصة هنا أن الخطر يتركز في عمليات التشفير بالمفتاح العام. والأخطر أن هذا النوع هو الذي يدير تبادل المفاتيح والهويات والتوقيعات (تحديد «من أنت؟» و«هل هذه المعاملة حقيقية؟») وهي أسئلة لا يقوم نظام مالي أو شبكة اتصالات بدونها.

هجوم «اجمع الآن، فُكّ لاحقًا Harvest Now, Decrypt Later» لماذا بدأ التهديد فعلاً؟

أكثر المفاهيم الخاطئة شيوعًا هو الاعتقاد بأن الخطر يبدأ فقط عند ظهور حاسوب كمي قادر على كسر الخوارزميات الحالية، لكن الحقيقة أن الخطر قد بدأ بالفعل. فالتقارير تشير إلى أن جهات استخباراتية وجماعات منظمة تعترض وتخزن اليوم كميات هائلة من البيانات المشفرة: لا لفكها الآن، بل انتظارًا حتى تصبح الحواسيب الكمية متاحة وتستطيع عندها كسر التشفير والوصول لها.

والمنطق بسيط، فالبيانات المشفرة المسروقة اليوم والمشفرة بخوارزميات RSA أو ECC ستصبح قابلة للفك مستقبلاً بخوارزمية شور. فإذا كانت هذه البيانات تحتاج سرية لمدة 15 سنة، والحاسوب الكمي سيظهر بعد 10 سنوات، فهذا يعني أنها ستصبح مكشوفة.

ويلخص الباحث ميشيل موسكا من جامعة واترلو بكندا المسألة بمعادلة بسيطة تعرف بـمبرهنة موسكا:

```
If X + Y > Z  {أنت في خطر الآن}
```

حيث:

- **X** = المدة التي تحتاج لبياناتك أن تبقى سرية خلالها مثلاً: سجلات طبية إو العقود
- **Y** = المدة التي ستستغرقها مؤسستك للتحول إلى تشفير ما بعد الكم، تاريخيًا: 10–20 سنة للتحولات التشفيرية الكبرى
- **Z** = المدة المتبقية حتى ظهور حاسوب كمي قادر على كسر خوارزميات التشفير الحالية (Q-Day)

فإذا كان مجموع عمر سرية البيانات وزمن الهجرة أطول من الزمن المتبقي حتى Q-Day، فالمشكلة قائمة اليوم وليست غدًا. وبما أن التحولات التشفيرية السابقة (مثل الانتقال من SHA-1 أو من DES) استغرقت أكثر من عقد من الزمن، فإن معظم المؤسسات الكبيرة تقع بالفعل داخل منطقة الخطر وهذا تحديدًا سبب إصرار الجهات التنظيمية على بدء الهجرة الآن رغم أن Q-Day قد يبدو بعيدًا عند البعض.

الأثر على الأنظمة المالية والبنوك

لا يوجد قطاع يستخدم التشفير بكثافة وتعقيد القطاع المالي، ولا يوجد قطاع تبقى بياناته قيّمة لفترات أطول: كالسجلات المصرفية التي تُحفظ لسنوات طويلة بحكم القانون، وهو ما يجعلها هدفًا مثاليًا لهجمات «أجمع الآن، فُكّ لاحقًا». والأهم أن الخطر في هذه الحالة (Systemic): فكسر التشفير لا يهدد معاملة واحدة، بل يقوض الثقة في النظام المالي بأكمله، فمن يستطيع تزوير التوقيعات يستطيع انتحال شخصية أي بنك أو إصدار أوامر دفع مزيفة لا تُميّز عن الأوامر الحقيقية.

أبرز النقاط المعرضة لهذا الخطر في البنية المالية:

النظام	دوره	طبيعة التعرض الكمومي
SWIFT ورسائل المدفوعات (ISO 20022)	أوامر الدفع بين البنوك عالميًا	تزوير أوامر الدفع؛ وصيغ الرسائل القديمة لم تُصمم لتوقيعات PQC الكبيرة
أنظمة التسوية الفورية (RTGS)	تسوية المدفوعات الكبرى بين البنوك المركزية والتجارية	خطر نظامي: اختراق واحد يهدد الاستقرار المالي كله
بطاقات الدفع وأجهزة الصراف	مصادقة البطاقات والمعاملات	شرائح وأجهزة منتشرة بملايين الوحدات يصعب تحديثها
أجهزة أمن العتاد (HSM)	حفظ المفاتيح السرية للبنوك	ليست كل الأجهزة قابلة للتحديث برمجيًا؛ استبدالها يستغرق وقت طويل
الخدمات المصرفية الرقمية وTLS	تطبيقات العملاء والخدمات المفتوحة (Open Banking)	اعتراض الجلسات وتخزينها لفكها لاحقًا. هجوم «أجمع الآن، فُكّ لاحقًا»
الأرشيف المالي طويل الأجل	سجلات تنظيمية تُحفظ لعقود	مكشوف بالكامل لهجوم «أجمع الآن، فُكّ لاحقًا»

تحديات عملية تجعل هجرة القطاع المالي أصعب من غيره:

- **حجم التوقيعات:** رسائل SWIFT التقليدية محدودة بـ 2,048 بايت، بينما توقيعات ما بعد الكم أكبر بكثير من توقيعات ECC الحالية، أي أن المشكلة ليست استبدال خوارزمية فقط بل إعادة تصميم صيغ الرسائل نفسها.
- **الترابط:** قيام بنك واحد بالإنتقال للخوارزميات الكمية لا يكفي؛ فالحماية تكتمل عندما ينتقل كذلك البنك المراسل ومزود شبكة المدفوعات والطرف المقابل أيضًا. وهذا يجعل المسألة تتطلب تنسيق بين منظومة كاملة، لا مؤسسة واحدة.
- **الضغط التنظيمي:** المنظمون في الولايات المتحدة وأوروبا (مثل لائحة DORA) وغيرهما بدأوا فعلًا بمطالبة المؤسسات المالية بجرد أصولها التشفيرية ووضع خطط انتقالها، فيما تستهدف SWIFT تجربة الرسائل المحمية بتشفير ما بعد الكم خلال السنوات القريبة القادمة.

الأثر على القطاعات الأخرى: كل ما يعتمد على الثقة الرقمية

التشفير بالمفتاح العام يمثل البنية التحتية الخفية لكل المنظومات الرقمية، والجدول التالي يوضح أين يقع التشفير في كل قطاع، وما الذي يتعرض للخطر، ومدى صعوبة التحديث:

القطاع	أين يعمل التشفير	ما الذي ينكسر	صعوبة التحديث
الاتصالات	شرائح SIM/eSIM، مصادقة شبكات 4G/5G، تشفير المكالمات	انتحال المشتركين، التنصت على الاتصالات، اختراق إدارة الشبكات	عالية — مليارات الشرائح والأجهزة المنتشرة
الهوية الرقمية	التوقيع الإلكتروني، الهويات الوطنية، أنظمة الدخول الموحد	انتحال الأشخاص والمؤسسات، تزوير الوثائق الموقعة	متوسطة — أنظمة مركزية نسبيًا
جوازات السفر الإلكترونية	شريحة الجواز موقعة رقميًا من الدولة المصدرة (معايير ICAO)	جوازات مزورة تجتاز الفحص الآلي	عالية جدًا — الجواز صالح 10 سنوات ولا يُحدّث بعد الإصدار
الطاقة والبنى الحيوية	أنظمة التحكم الصناعي (SCADA)، الشبكات الذكية	أوامر تحكم مزيفة في محطات الكهرباء والمياه	عالية — أجهزة تعمل لعقود دون تحديث
الصحة	السجلات الطبية، الأجهزة الطبية المتصلة	كشف بيانات حساسة تبقى سرية مدى الحياة، التلاعب بالأجهزة	متوسطة إلى عالية
إنترنت الأشياء والسيارات	تحديثات البرمجيات الموقعة، مفاتيح السيارات، الأجهزة المنزلية	تحديثات خبيثة تبدو شرعية، التحكم بالأجهزة عن بعد	عالية جدًا — أجهزة رخيصة بلا قدرة حسابية لخوارزميات أكثر تعقيداً
الحكومة والدفاع	الاتصالات المصنفة، الوثائق الرسمية	كشف أسرار الدولة المخزنة منذ سنوات	جارٍ بالفعل — أعلى أولوية رسمية

وكما نلاحظ فإن النمط المشترك يتمثل في أنه كلما طال عمر الجهاز أو الوثيقة (جواز سفر 10 سنوات، سيارة 15 سنة، محطة طاقة 30 سنة)، كان لزامًا أن يُدمج تشفير ما بعد الكم في تصميمه في مرحلة أبكر، لأن ما يُصدر اليوم سيظل في الخدمة بعد Q-Day.

العملات المشفرة والبلوك تشين: قطاع أكثر هشاشة

إذا كانت البنوك تستطيع تجميد المعاملات وإصدار بطاقات جديدة عند اكتشاف اختراق، فإن العملات المشفرة لا تملك هذا الخيار: لا سلطة مركزية تستطيع إلغاء معاملة أو استبدال مفتاح. المفتاح الخاص هو الملكية، ومن يستطيع اشتقاقه من المفتاح العام بخوارزمية شور يملك هذه الأموال حسب نظر بروتوكول الشبكة.

فتقريبًا كل العملات الكبرى (بيتكوين، إيثريوم وغيرها) تستخدم توقيعات ECDSA على منحنى secp256k1 — وهو بالضبط ما تكسره خوارزمية شور. وقد نشر فريق Google Quantum AI في مارس 2026 ورقة تقدر أن كسر هذا المنحنى قد يتطلب أقل من 500 ألف كيوبت فيزيائي ودقائق معدودة من التشغيل على معماريات فائقة التوصيل وهذه أرقام أقل بكثير مما كان مفترضًا قبل سنوات.

سطحا الهجوم الرئيسيان

1. **الهجوم طويل المدى (على الأموال الساكنة):** أي عنوان كُشف مفتاحه العام على السلسلة (عناوين بيتكوين القديمة P2PK، والعناوين المعاد استخدامها، وكل حسابات إيثريوم النشطة والتي قامت على الأقل بإرسال معاملة واحدة) معرض لسرقة أمواله فور ظهور حاسوب كمي قادر. وهذا يشمل نحو مليون بيتكوين منسوبة لساتوشي ناكاموتو لا يمكن نقلها كون صاحبها غير معروف.

2. **الهجوم قصير المدى (على المعاملات الحية):** عند إرسال أي معاملة يُكشف المفتاح العام في الذاكرة المؤقتة (mempool). وبوجود حاسوب كمي سريع بما يكفي لاشتقاق المفتاح الخاص خلال دقائق التأكيد (نحو 10 دقائق في بيتكوين) يستطيع سرقة أي معاملة قبل تأكيدها، مما يجعل الشبكة كلها غير صالحة للاستخدام.

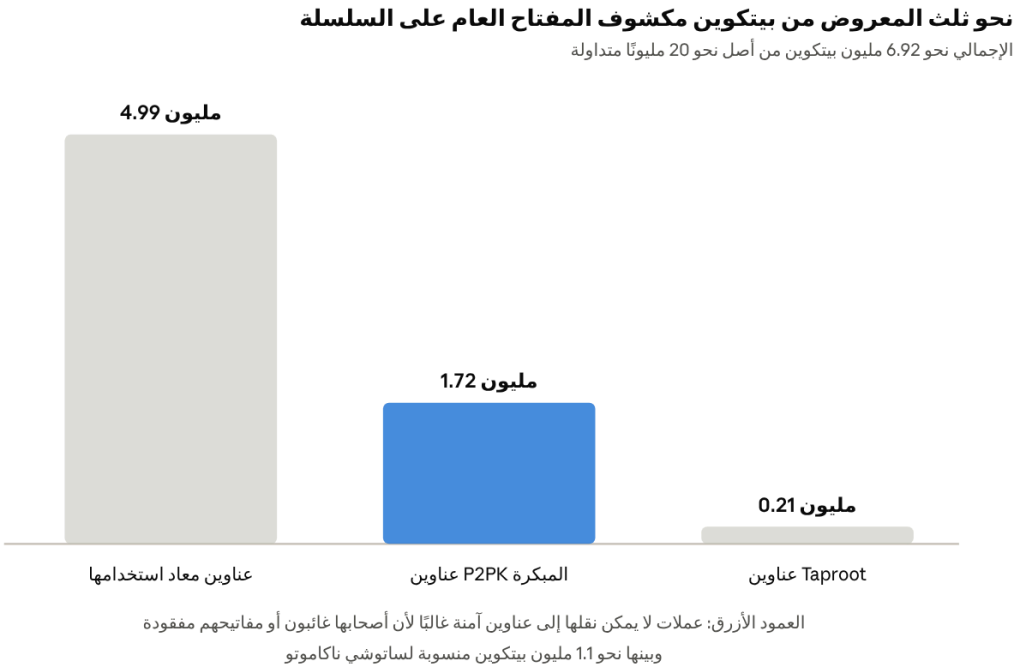
بيتكوين مقابل إيثريوم: نهجان مختلفان

المحور	بيتكوين	إيثريوم
الحوكمة	لا مؤسسة ولا خارطة طريق رسمية؛ تغييرات بطيئة بالإجماع	مؤسسة إيثريوم أعلنت أمن ما بعد الكم كأولوية واستراتيجية عليا (2026) مع فريق مخصص وجوائز بحثية لتطوير ذلك
الخطة المعلنة	مقترحات متفرقة مثل BIP-360 وBIP-361 لعناوين وأوامر برمجية مقاومة للكم (2025–2026)	مركز pq.ethereum.org (مارس 2026): خارطة طريق مرحلية تستبدل طبقات التشفير تدريجيًا (تنفيذ، إجماع، بيانات)
حجم التعرض	نحو 20–30% من العملة في عناوين مكشوفة المفتاح	كل الحسابات النشطة مكشوفة المفتاح بحكم التصميم، لكن المرونة التشفيرية وتجريد الحسابات يسهلان الترقية
الأدوات المقترحة	توقيعات هاش (WOTS، SLH-DSA+) أو ML-DSA عبر تحديث ناعم (soft fork)	ML-DSA، توقيعات هاش، ونهج هجين «1 من 2» يقبل التوقيع التقليدي أو الكمي أثناء الانتقال

التحدي الفريد هنا ليس تقنيًا فقط بل يعتمد على المجتمع المكون لهذه الشبكات: الهجرة تتطلب من كل مالك أن ينقل أمواله بنفسه إلى عنوان مقاوم للكم، والأموال التي لن تنتقل (مفاتيح مفقودة، أصحاب غائبون) ستظل غنيمة مؤجلة لأول حاسوب كمي قادر. كما أن مسألة «ماذا نفعل بأموال ساتوشي؟» — هل تُحرق برمجيًا أم تُترك للسرقة؟ — ستكون من أكثر النقاشات انقسامًا في تاريخ بيتكوين.

كم بيتكوين معرّض فعلاً للخطر؟

التحليلات الحديثة لسلسلة بيتكوين (Checkonchain وتقرير المجلس الاستشاري لـ Coinbase، 2026) تتقارب عند رقم عالي ويتمثل في نحو **6.9 مليون بيتكوين**، أي قرابة ثلث المعروض والمتداول، ومئات المليارات من الدولارات بأسعار اليوم موجودة في عناوين مفاتيحها العامة مكشوفة بالفعل على السلسلة، أي أنها قابلة للسرقة نظريًا فور ظهور حاسوب كمي قادر على تشغيل خوارزمية شور بفعالية عالية.



بيانات Bitcoin Research Kit عبر Checkonchain وتقرير المجلس الاستشاري لـ Coinbase (2026)

تفصيل الفئات الثلاث:

- **عناوين P2PK المبكرة (نحو 1.72 مليون):** صيغة العناوين الأولى في 2009–2010 كانت تضع المفتاح العام نفسه في العنوان مباشرة. معظمها ساكن منذ أكثر من عقد، وبينها نحو 1.1 مليون بيتكوين منسوبة لساتوشي. هذه الفئة لا يمكن إنفاذها إطلاقًا دون تدخل أصحابها الغائبين، لأن النقل إلى عنوان آمن يتطلب المفتاح الخاص.
- **العناوين المعاد استخدامها (نحو 5 ملايين):** العناوين الحديثة تخفي المفتاح العام خلف دالة هاش — لكن أول عملية إنفاق من العنوان تكشفه للأبد. من يستقبل أموالاً على عنوان سبق الإنفاق منه يصبح مكشوفًا. الجانب الإيجابي: معظم هذه الفئة لدى منصات تداول وجهات حفظ تستطيع نقلها إلى عناوين جديدة بقرار إداري واحد.
- **عناوين Taproot (نحو 0.21 مليون):** أحدث صيغة (2021) تعيد للمفارقة كشف المفتاح العام بحكم التصميم.

وتضيف ورقة Google Quantum AI تفصيلة مهمة: نحو 2.3 مليون بيتكوين مكشوفة وساكنة معًا (لم تتحرك منذ خمس سنوات على الأقل) وهذه هي الغنيمة الحقيقية المؤجلة. فهي أموال لن ينقلها أحد لأن أصحابها غائبون أو متوفون أو فقدوا مفاتيحهم، وسرقتها الصامتة قد لا تُكتشف إلا بعد فوات الأوان.

إيثريوم: أين تكمن المشكلة؟

إيثريوم لا يستخدم نموذج العناوين المستهلكة مرة واحدة كبيتكوين، بل نموذج «الحسابات»: حساب واحد ثابت تخرج منه كل معاملاتك. النتيجة: أول معاملة ترسلها تكشف مفتاحك العام للأبد، أي أن كل الحسابات النشطة تقريبًا مكشوفة بحكم التصميم ونسبة تعرض أعلى من بيتكوين. وتتسع الهشاشة لأسطح إضافية لا وجود لها في بيتكوين:

- **العقود الذكية وأموال DeFi:** مليارات الدولارات المقفلة في بروتوكولات مثل Uniswap وAave وMaker تحتاج كل منها خطة انتقال خاصة.
- **توقيعات المدققين (BLS):** طبقة الإجماع نفسها تستخدم توقيعات معرضة كميًا ويجب استبدالها.
- **في المقابل، يملك إيثريوم ميزة مهمة:** المرونة التشفيرية ونظام الحسابات المعروف ب (Account Abstraction) يسمحان لكل حساب بتغيير خوارزمية توقيعه دون تغيير عنوانه وهو ما يجعل الترقية أسهل هندسيًا رغم اتساع سطح التعرض.

الحلول المقترحة لكل شبكة

الشبكة	المقترح	الفكرة ببساطة
بيتكوين	(BIP-360 (P2QRH	نوع عنوان جديد مقاوم للكم يزيل مسار المفتاح المكشوف من Taproot
بيتكوين	(BIP-361 (2026	أوامر برمجية لتوقيعات ما بعد الكم عبر تحديث ناعم، مع نقاش تقييد الإنفاق من العناوين المكشوفة تدريجيًا
بيتكوين	حلول الطبقة الثانية	محافظ بتوقيعات هاش (مثل WOTS+) فوق الشبكة الحالية دون انتظار الإجماع
بيتكوين	معضلة التجميد	نقاش مفتوح: هل تُجمد العملات المكشوفة غير المهاجرة برمجيًا أم تُترك لأول سارق كمومي؟ لا إجماع بعد
إيثريوم	مسبقات ML-DSA + تجريد الحسابات	دعم توقيعات NIST ما بعد الكم على مستوى البروتوكول، وكل مالك حساب يقوم بتبديل الخوارزمية بنفسه
إيثريوم	النهج الهجين «1 من 2»	الحساب يقبل التوقيع التقليدي أو الكمومي خلال الانتقال، فتتم الترقية تدريجيًا بلا كلفة فورية على المستخدم
إيثريوم	leanVM والبراهين المعتمدة على الهاش (STARKs)	إعادة بناء طبقات الإثبات على دوال هاش آمنة كميًا بطبيعتها وهو حجر الأساس في خارطة الطريق

أما على مستوى المستخدم الفرد فالتوصية العملية اليوم بسيطة: لا تُعد استخدام العناوين أبدًا — استقبل كل دفعة على عنوان جديد — فهذا وحده يُخرج أموالك من فئة الخطر الفوري إلى أن تتوفر العناوين المقاومة للكم رسميًا.

الحل: معايير NIST لتشفير ما بعد الكم (PQC)

الجانب الجيد هو أن الحل موجود ومعتمد رسميًا. فتشفير ما بعد الكم (Post-Quantum Cryptography) لا يحتاج حاسوبًا كميًا هو تشفير تقليدي يمكن أن يعمل على الأجهزة الحالية، لكنه مبني على مسائل رياضية مختلفة (مثل الشبيكات Lattices ودوال الهاش) ولا تعرف الحواسيب الكمية طريقة فعالة لحلها.

وبعد مسابقة عالمية استمرت 8 سنوات (2016–2024) وشاركت فيها فرق بحثية من أنحاء العالم، نشر المعهد الوطني الأمريكي للمعايير والتقنية (NIST) أول ثلاثة معايير نهائية في أغسطس 2024، ثم اختار خوارزمية خامسة (HQC) في مارس 2025:

المعيار	الخوارزمية	الأساس الرياضي	الوظيفة	الحالة	تحل محل
FIPS 203	ML-KEM (اسمها السابق Kyber)	الشبيكات	تبادل المفاتيح	منشور (أغسطس 2024) — المعيار الأساسي	RSA، ECDH، Diffie-Hellman
FIPS 204	ML-DSA (اسمها السابق Dilithium)	الشبيكات	التوقيعات الرقمية	منشور (أغسطس 2024) — المعيار الأساسي	RSA، ECDSA
FIPS 205	SLH-DSA (اسمها السابق SPHINCS+)	دوال الهاش	توقيعات احتياطية (أكبر حجمًا لكن بأساس رياضي مختلف)	منشور (أغسطس 2024)	RSA، ECDSA

المعيار	الخوارزمية	الأساس الرياضي	الوظيفة	الحالة	تحل محل
FIPS 206	FN-DSA (اسمها السابق Falcon)	الشبيكات	توقيعات مدمجة الحجم	مسودة قيد الإعداد	ECDSA في التطبيقات محدودة المساحة
—	HQC	الشفرات (Codes)	تبادل مفاتيح احتياطي	اختيرت مارس 2025؛ المعيار النهائي متوقع نحو 2027	بديل لـ ML-KEM

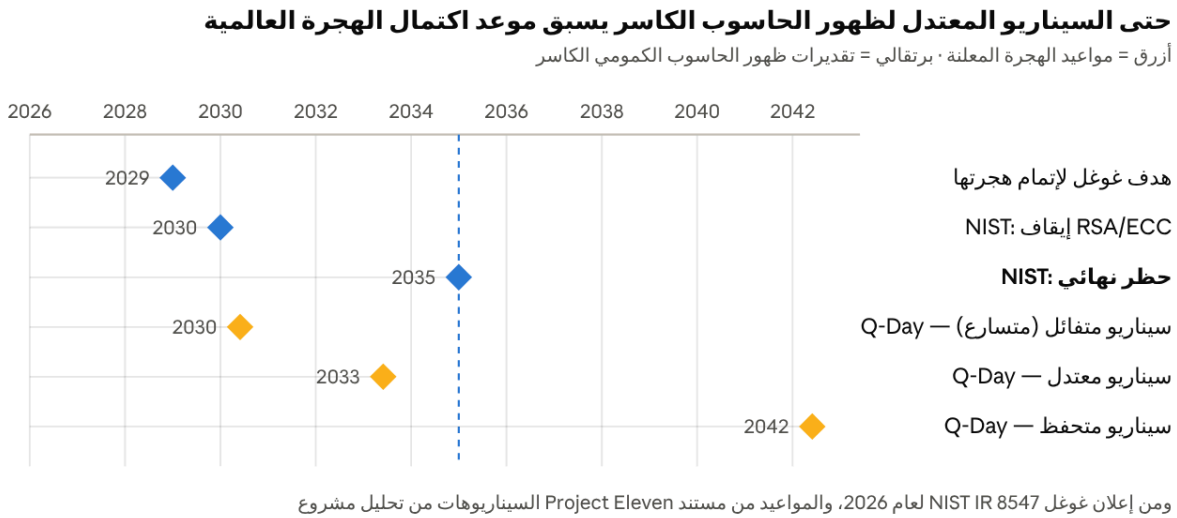
ملاحظتان مهمتان:

- **لماذا أكثر من خوارزمية؟** التنويع مقصود بحيث لو اكتُشفت ثغرة في أساس الشبيكات مستقبلاً، تبقى خوارزميات الهاش والشفرات سليمة. وهذا درس مستفاد من المسابقة نفسها فخوارزمية SIKE المرشحة كُسرت عام 2022 على حاسوب محمول عادي.
- **التكلفة العملية:** مفاتيح وتوقيعات PQC أكبر بكثير من نظيرتها الحالية (مفتاح ML-KEM-768 العام نحو 1,184 بايت مقابل 32 بايت لـ X25519)، ما يزيد حجم الاتصالات ويسبب تحديات حقيقية للأجهزة الصغيرة والبروتوكولات محدودة الحجم لكنها تكلفة مقبولة مقابل أمن الشبكة والمعلومات.

متى يحل يوم Q-Day؟ السيناريوهات والتوقعات

Q-Day هو اليوم الذي يوجد فيه حاسوب كمي قادر عمليًا على كسر التشفير بالمفتاح العام المستخدم اليوم. ولا أحد يعرف هذا التاريخ بدقة، والتقديرات تتراوح بين من يعتقد أنه قد حدث سرًا في مختبر مصنف أو أنه لن يحدث أبدًا، ولكن إجماع الخبراء يتركز على أنه سيحدث في الثلاثينيات من هذا القرن.

وأحدث الأرقام الموثوقة تتمثل في تقرير «الجدول الزمني للتهديد الكمومي» السابع (مارس 2026) من معهد المخاطر العالمي بإشراف ميشيل موسكا، الذي استطلع 26 خبيرًا عالميًا، ويقدر احتمال ظهور CRQC خلال 10 سنوات بين 28% و48% تقريبًا وهي أعلى نسبة في تاريخ تتبع هذا الأمر ويراه الخبراء مرجحًا خلال 15 سنة. سبب ارتفاع هذه النسبة في التقديرات الحديثة (مثل ورقة الباحث كريغ غيدني من غوغل) كونها قد خفضت عدد الكيوبتات اللازمة لكسر RSA-2048 إلى أقل من مليون كيوبت فيزيائي.

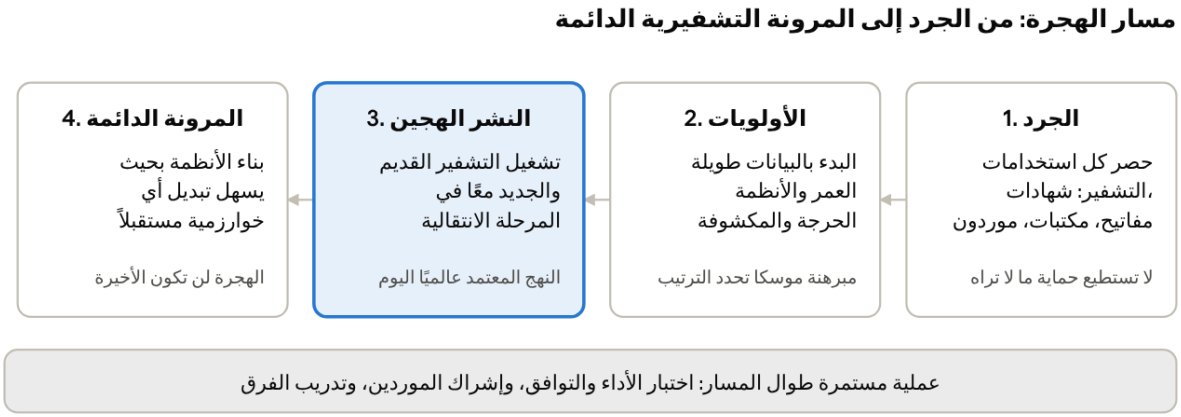


سيناريوهات Q-Day مقابل مواعيد الإنتقال المعلنة · مصادر: Google 2026، NIST IR 8547، Project Eleven

والرسالة الحرجة والمهمة التي يحملها الرسم أعلاه هي جوهر المسألة كلها. ففي السيناريو المتسارع يمكن أن يصل Q-Day قبل أن تُكمل معظم المؤسسات هجرتها، وحتى في السيناريو المعتدل (2033) يسبق الموعد النهائي العالمي لإتمام الهجرة (2035). ويضيف عالم الرياضيات في NIST داستن مودي ملاحظة حاسمة فحتى لو ظهر الحاسوب الكمي بعد خمس سنوات فقط، فإن الانتقال العالمي لن يكون قد اكتمل، إذ استغرقت التحولات التشفيرية السابقة من 10 إلى 20 سنة. كما توجد نقطة أخيرة يحذر منها التقرير نفسه، بأن Q-Day الحقيقي قد يقع قبل أن يعلم العالم به، فالدولة أو الجهة التي تصل أولاً من المرجح أنها ستستخدم هذه التقنية بصمت لصالحها الاستراتيجي بدل الإعلان عنها مباشرة.

مسار الإنتقال: كيف ننتقل إلى تشفير ما بعد الكم؟

من المهم في كل المؤسسات إدراك أن الإنتقال ليس تحديث برنامج، بل هو مشروع تحول مؤسسي متعدد السنوات يمس كل نظام وبروتوكول وجهاز ومورد. والمسار المتفق عليه عالميًا يمر بأربع مراحل:



المراحل الأربع لإنتقال المؤسسات إلى تشفير ما بعد الكم

تفصيل المراحل:

1. **الجرد التشفيري (Cryptographic Inventory):** حصر كل مواضع استخدام التشفير في المؤسسة: الشهادات، المفاتيح، المكتبات البرمجية، البروتوكولات، واعتماديات الموردين. معظم المؤسسات تُفاجأ بأنها لا تعرف أين يعيش تشفيرها أصلاً. النتيجة تسمى «فاتورة المواد التشفيرية» (CBOM).
2. **تقييم المخاطر وتحديد الأولويات:** تطبيق مبرهنة موسكا على كل نظام: البيانات طويلة العمر المعرضة للاعتراض أولاً (اتصالات خارجية، أرشيف حساس)، ثم الأنظمة الحرجة، ثم البقية.
3. **النشر الهجين (Hybrid):** تشغيل الخوارزمية التقليدية وخوارزمية ما بعد الكم معًا في العملية نفسها (مثل X25519 MLKEM768 في TLS): إذا ثبت ضعف إحداهما تبقى الأخرى حامية للنظام، وهذا هو النهج الذي تعتمده المتصفحات والبنوك وتوصي به الجهات التنظيمية للمرحلة الانتقالية.
4. **المرونة التشفيرية (Crypto-Agility):** إعادة بناء الأنظمة بحيث تصبح الخوارزمية مكونًا قابلاً للاستبدال دون إعادة هندسة. الدرس الأعمق من هذه الأزمة هو أن خوارزميات PQC نفسها قد تحتاج للإستبدال يومًا ما.

أما الجدول الزمني التنظيمي الحاكم عالميًا فيحدده بشكل أساسي مستند NIST IR 8547 وخطة وكالة الأمن القومي الأمريكية CNSA 2.0 وخارطة طريق الاتحاد الأوروبي وهو مسرود في الجدول أدناه:

الموعد	الحدث
2024	نشر المعايير النهائية (FIPS 203/204/205) — بدء التبني الفعلي
بنهاية 2026	كل دولة في الاتحاد الأوروبي تملك استراتيجية وطنية لـ PQC
2027	اشتراط توافق المشتريات الجديدة لأنظمة الأمن القومي الأمريكية مع CNSA 2.0
2029	هدف غوغل المعلن لإتمام هجرة أنظمتها
2030	NIST: إيقاف (deprecate) RSA-2048 وECC P-256؛ اكتمال هجرة البنى الحرجة في الاتحاد الأوروبي؛ أستراليا توقف RSA/ECC نهائيًا
2033–2031	CNSA 2.0 إلزامي تدريجيًا عبر فئات المنتجات (شبكات، أنظمة تشغيل، خدمات سحابية)
2035	حظر نهائي (disallow) لكل الخوارزميات المعرضة كميًا في معايير NIST؛ اكتمال الهجرة الأوروبية وأنظمة الأمن القومي الأمريكية

من يفعل ماذا؟ خريطة الجهود العالمية

التحول بدأ فعلًا وبوتيرة متسارعة والمؤشر الأوضح أن أكثر من ثلثي حركة التصفح عبر شبكة كلاودفلير تستخدم اليوم تبادل مفاتيح هجينًا مقاومًا للكم دون أن يشعر المستخدمون بشيء.

الجهة	ماذا تفعل	الحالة
NIST (الولايات المتحدة)	نشر المعايير (FIPS 203/204/205) وجدول الإيقاف (IR 8547)	المعايير منشورة؛ المواعيد ملزمة فعليًا للجهات الفدرالية
وكالة الأمن القومي NSA	حزمة CNSA 2.0 لأنظمة الأمن القومي: إلزام تدريجي 2027–2033	جارٍ
الاتحاد الأوروبي	خارطة طريق منسقة (يونيو 2025): استراتيجيات وطنية بنهاية 2026، البنى الحرجة 2030، الكل 2035	جارٍ؛ لائحة DORA تضغط على القطاع المالي
غوغل	متصفح Chrome يستخدم ML-KEM الهجين افتراضيًا منذ 2024؛ أعلنت جوجل عام 2029 كهدف لإتمام هجرة أنظمتها	منشور ومُفعّل
أبل وسيغنال	iMessage ببروتوكول PQ3 وSignal ببروتوكول PQXDH: رسائل محمية كموميًا لمليارات المستخدمين	مُفعّل منذ 2023–2024
كلاودفلير ومزودو البنى السحابية	تفعيل التبادل الهجين على حافة الشبكة؛ أكثر من ثلثي الحركة البشرية محمية (أبريل 2026)	مُفعّل ومتسارع
القطاع المالي (SWIFT والبنوك الكبرى)	تجارب رسائل محمية بـ PQC، جرد تشفيري بضغط تنظيمي أمريكي وأوروبي وبريطاني	مرحلة التجارب والجرد

الجهة	ماذا تفعل	الحالة
مؤسسة إيثريوم	فريق PQ مخصص + جوائز بحثية 2 مليون دولار + مركز pq.ethereum.org بخارطة طريق مرحلية	أعلن كأولوية عليا (2026)
مجتمع بيتكوين	مقترحات BIP-360/BIP-361 لعناوين وتوقيعات مقاومة للكم	نقاش مجتمعي دون خطة ملزمة حتى الآن
دول أخرى (أستراليا، سنغافورة، كوريا، كندا، الإمارات وغيرها)	استراتيجيات وطنية للأمن الكمي بمواعيد متفاوتة؛ أستراليا الأكثر تشددًا (إيقاف RSA/ECC بنهاية 2030)	منشورة وجاري العمل عليها

ومن المهم ملاحظة أن الفجوة المقلقة في هذه الخريطة ليست في المتصفحات ولا الحكومات الكبرى، بل في طبقة الخوادم والمؤسسات المتوسطة (نسبة الخوادم الأصلية المدعومة ما تزال ضئيلة)، وفي الدول التي لم تضع بعد أي استراتيجية وطنية وهي فجوة تستحق اهتمامًا خاصًا في منطقتنا العربية، إذ ستستورد معظم دولها التحول عبر الموردين العالميين دون خطة سيادية تحكم أولوياتها.

الخدمات الحكومية: ماذا يتأثر، وكم تخطط الحكومات للإنفاق؟

الحكومات هي أكبر مستخدم منفرد للتشفير بالمفتاح العام، وكل خدمة رقمية تقدمها تقوم عليه: بوابات الضرائب والجمارك، والهوية الوطنية والتوقيع الإلكتروني على الوثائق الرسمية، والسجلات الصحية والضمان الاجتماعي، وأنظمة المحاكم والسجل العقاري، والاتصالات الدبلوماسية والعسكرية، وصولاً إلى العملات الرقمية للبنوك المركزية مستقبلاً. والأرشيف الحكومي تحديدًا — بيانات تعداد ومراسلات وملفات أمنية تبقى سرية لعقود — هو الهدف الأول لهجمات «اجمع الآن، فُكّ لاحقًا»، ولهذا تتحرك الحكومات قبل القطاع الخاص لا بعده. الجدول التالي يلخص أبرز الخطط والموازنات المعلنة:

الحكومة	الإطار والخطة	الإنفاق والموارد المعلنة
الولايات المتحدة (الوكالات المدنية)	مذكرة NSM-10 (2022) + قانون الجاهزية الكمومية: جرد سنوي، هجرة الأنظمة ذات الأولوية 2025–2035	تقدير رسمي من البيت الأبيض: نحو 7.1 مليار دولار (بدولار 2024) للفترة 2025–2035، والجزء الأكبر لاستبدال الأنظمة القديمة غير القابلة للتحديث
الولايات المتحدة (الدفاع والاستخبارات)	حزمة CNSA 2.0 إلزامية تدريجيًا لأنظمة الأمن القومي حتى 2033	تقديرات تمويل منفصلة (غير منشورة علنًا) تُضاف فوق الـ 7.1 مليار
المملكة المتحدة	خارطة طريق مركز الأمن السيبراني NCSC: اكتشاف وجرد بحلول 2028، هجرة الأنظمة ذات الأولوية بحلول 2031، اكتمال الهجرة بحلول 2035	إرشاد إلزامي الطابع للقطاعات الحيوية؛ التمويل ضمن موازنات الجهات
الاتحاد الأوروبي	خارطة الطريق المنسقة (2025): استراتيجية وطنية لكل دولة بنهاية 2026، البنى الحيوية 2030، الجميع 2035؛ تُعتبر أشمل نهج تنسيقي عابر للدول	تمويل موزع على الدول الأعضاء وبرامج الاتحاد الرقمية؛ لائحة DORA تنقل كلفة الامتثال للقطاع المالي نفسه
أستراليا	دليل ASD: إيقاف RSA وECC وDH نهائيًا بنهاية 2030 — أكثر الجداول تشددًا عالميًا	ضمن موازنات الأمن السيبراني الوطنية
دول أخرى (سنغافورة، كوريا، كندا، الإمارات)	استراتيجيات أمن كمومي وطنية منشورة بمواعيد مؤسسية	متفاوت؛ الإمارات أدرجت PQC صراحة في سياسات مجلس الأمن السيبراني

الخلاصة والتوصيات

التهديد الكمي قد لا يمثل نهاية العالم الرقمي، ولكنه بالتأكيد سيكون من أكبر عمليات استبدال للبنية التحتية الأمنية في تاريخ الإنترنت. ومن يبدأ مبكرًا ينتقل بهدوء، ومن ينتظر سيدفع تكلفة الهجرة المتعجلة وثمن بياناته التي تم تجميعها مسبقاً.

1. التشفير بالمفتاح العام (RSA/ECC) سيكسر بالكامل؛ التشفير المتماثل (AES-256) ودوال الهاش ستصمد.
2. هجوم «أجمع الآن، فُكّ لاحقًا» يجعل التهديد قائمًا منذ اليوم على كل البيانات طويلة العمر.
3. الحلول موجودة ومعتمدة (معايير NIST) ومُفعّلة بالفعل في متصفحك منذ الآن، والمتأخر هو طبقة المؤسسات والخوادم والأجهزة المُعمّرة.
4. المواعيد التنظيمية (2030 إيقاف، 2035 حظر) أصبحت الساعة الفعلية التي تحكم القرار بغض النظر عن موعد Q-Day الحقيقي.
5. العملات المشفرة أكثر الأنظمة هشاشة لغياب سلطة مركزية تفرض الترقية، وهجرتها مسألة حوكمة بقدر ماهي مسألة تقنية.

وختاماً فالخطوة الأولى لأي مؤسسة واحدة لا تتغير: البدء بعمليات الجرد التشفيري اليوم، وسؤال كل مورد يتم التعامل معه منذ اليوم سؤال واحد ومهم حول ما هي خطة المورد لدعم تشفير ما بعد الكم، ومتى؟.

المصادر والمراجع

- NIST — مشروع توحيد تشفير ما بعد الكم (FIPS 203/204/205، HQC)
- NIST IR 8545 — تقرير الجولة الرابعة واختيار HQC
- تقرير الجدول الزمني للتهديد الكمومي 2025/2026 — موسكا وبياني، معهد المخاطر العالمي
- تقرير Project Eleven — سيناريوهات توقع Q-Day
- مواعيد الهجرة: NIST IR 8547 و The Quantum Insider — CNSA 2.0
- تحليل PostQuantum.com — NIST IR 8547
- خارطة طريق الاتحاد الأوروبي لـ PQC (يونيو 2025)
- تبني PQC في المتصفحات ونسب الحركة المحمية — Encryption Consulting
- التهديد الكمومي للعملات المشفرة وتقديرات Google Quantum AI لكسر secp256k1
- بيتكوين وإيثريوم أمام هدف غوغل 2029 — QRL
- الانقسام الكمومي بين بيتكوين وإيثريوم — Cointelegraph
- توصيات المجلس الاستشاري لـ Coinbase حول الترقيات الكمومية (أبريل 2026)
- تشفير ما بعد الكم في القطاع المالي — مراجعة علمية (arXiv)
- تحديات هجرة القطاع المالي (حدود ISO 8583 وSWIFT وأجهزة HSM) — Encryption Consulting
- تبني PQC في TLS عمليًا (Signal، iMessage PQ3، Cloudflare، Chrome)
- تفصيل البيتكوين المكشوف كموميًا (P2PK وإعادة الاستخدام و Taproot) — Checkonchain
- تقرير المجلس الاستشاري لـ Coinbase: نحو 7 ملايين بيتكوين معرضة
- هشاشة بيتكوين الكمومية وتقديرات العملات الساكنة — PostQuantum.com
- تحليل ديلويت: الحواسيب الكمومية وسلسلة بيتكوين
- تقرير البيت الأبيض: 7.1 مليار دولار لهجرة الوكالات الفدرالية — The Quantum Insider
- دراسة سياسات تنفيذ PQC: فجوات الموازنات والجرد (2026)