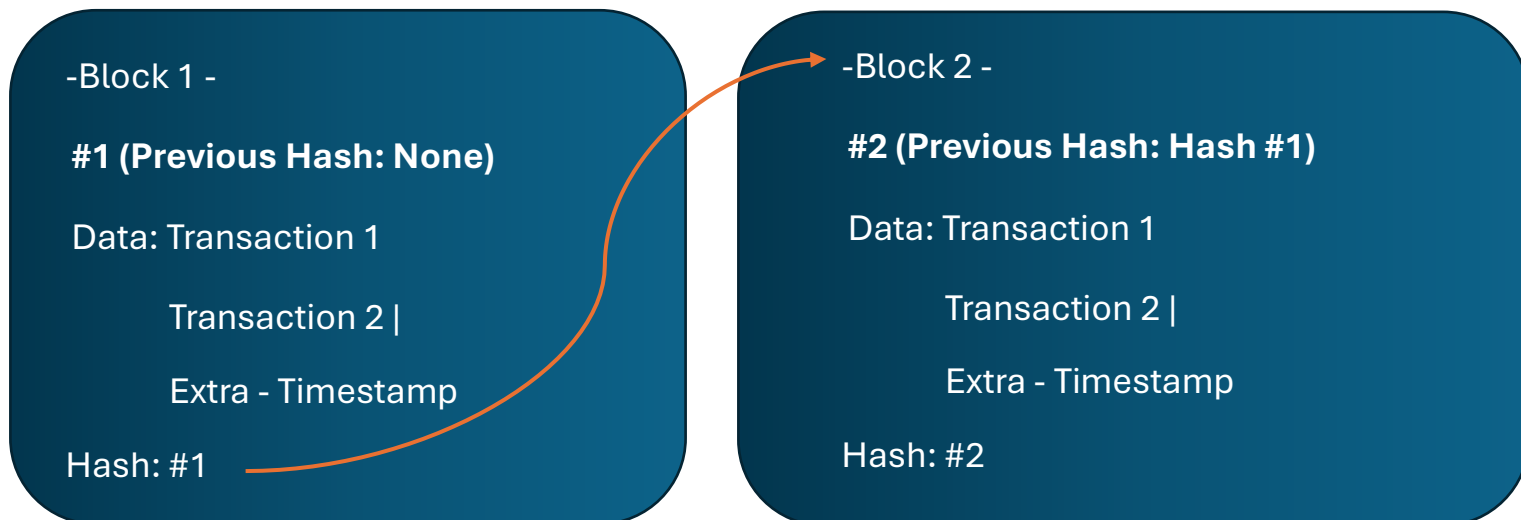


ماهو Blockchain ؟

ال Blockchain هو سجل رقمي موثّق وغير قابل للتعديل يُستخدم لتخزين البيانات بشكل آمن وشفاف، ويتكوّن من سلسلة من الكتل، كل كتلة تحتوي على مجموعة من المعاملات وتكون مرتبطة بالكتلة السابقة عبر رمز تشفيري (هاش)، مما يجعل أي محاولة للتلاعب صعبة جدًا. يتم نسخ هذا السجل عبر شبكة من الأجهزة (العُقد)، ويُدار من خلال آليات توافق مثل Proof of Work لضمان صحة البيانات دون الحاجة لوسيط مركزي. تُستخدم تقنية البلوكشين في تطبيقات متعددة، أبرزها العملات الرقمية مثل Bitcoin ، والعقود الذكية، وسلاسل التوريد، والتصويت الإلكتروني.



في الحاسوب الكمي هناك مصطلحان مهمان هما :

1. التراكب الكمي Superposition

في الحوسبة الكمية، البت الكمي (qubit) يمكن أن يكون في الحالتين 0 و 1 في نفس الوقت، وليس فقط واحدة منهما كما في الحوسبة التقليدية. هذا ما يسمى التراكب، ويمنح الحاسوب الكمي قدرة على معالجة معلومات أكثر بكثير في وقت واحد.

2. التشابك الكمي Entanglement

هو ارتباط بين qubits بحيث أن تغيير حالة أحدهما يؤثر مباشرة على الآخر، مهما كانت المسافة بينهما. هذا يتيح تنفيذ عمليات كمية معقدة بسرعة وكفاءة عالية.

خوارزمية Shor:

هي خوارزمية في الحوسبة الكمية تُستخدم لتحليل الأعداد الكبيرة إلى عواملها الأولية بسرعة كبيرة، وضعها العالم Peter Shor سنة 1994 وهي تُعد تهديدًا لأنظمة التشفير التقليدية مثل RSA التي تعتمد على صعوبة هذه العملية.

نجد أن عوامل 15 هي $3 * 5$

مقارنه بين AES و SHA-256

المعيار	SHA-256	AES
النوع	خوارزمية تجزئة (Hashing)	خوارزمية تشفير (Encryption)
الغرض	إنشاء بصمة رقمية ثابتة لبيانات	تشفير البيانات وفكّها
الاتجاه	اتجاه واحد (لا يمكن عكسه)	اتجاهين (تشفير وفك التشفير)
الوظيفة الأساسية	التأكد من سلامة البيانات	حماية سرية البيانات
المفتاح	لا يستخدم مفتاحًا	يستخدم مفتاح تشفير (128, 192, أو 256 بت)
الإخراج	ناتج دائم طوله 256 بت	ناتج بطول يساوي البيانات المُشفّرة
الاستخدامات	التوقيع الرقمي، التحقق من البيانات	حماية الملفات، الاتصالات، البيانات الحساسة
الأمان	قوي، غير قابل للعكس	قوي جدًا إذا استُخدم بمفتاح طويل

مقارنة بين الحاسوب الكمي و الحاسوب العادي

المعيار	الحاسوب العادي (الكلاسيكي)	الحاسوب الكمي
الوحدة الأساسية	0 Bit أو 1 فقط	Qubit 0 و 1 في نفس الوقت - تراكب

يعتمد على ميكانيكا الكم (تراكب وتشابك)	يعتمد على الجبر التقليدي والتسلسل	طريقة العمل
هائلة في مهام معينة (مثل تحليل الأعداد، البحث)	خطية، محدودة بالمعالج والذاكرة	القوة الحسابية
يمكن تنفيذ عمليات متوازية على عدة حالات في وقت واحد	تنفذ واحدة تلو الأخرى	العمليات
التشفير، الكيمياء الكمّية، الذكاء الاصطناعي المتقدم	المهام اليومية، البرمجة، الإنترنت، الألعاب	الاستخدامات
لا يزال في مرحلة البحث والتطوير	مستقر ومستخدم على نطاق واسع	درجة النضج
عرضة للأخطاء الكمّية، تصحيحها صعب ومعقد	نادر نسبياً، سهل التصحيح	الأخطاء والتصحيح

مقارنة بين التشفير العادي و تشفير باستخدام Blockchain

المعيار	التشفير العادي	التشفير باستخدام Blockchain
الهدف	حماية البيانات أثناء النقل أو التخزين	توثيق المعاملات وحمايتها من التزوير ضمن سجل مشفّر
الطريقة	يستخدم خوارزميات مثل AES ، RSA	يستخدم التشفير ضمن هيكل سلاسل الكتل وتوقيع رقمي
المفتاح	يحتاج مفتاح (سري أو عام/خاص)	يستخدم مفاتيح عامة وخاصة لتوقيع وتوثيق المعاملات
الوظيفة	تشفير وفك تشفير البيانات	توثيق المعاملات بطريقة لا يمكن تعديلها
الاتجاه	اتجاهين (تشفير وفك التشفير)	غالبًا اتجاه واحد (توقيع وتسجيل دائم للبيانات)
المرونة	مرن ويمكن استخدامه مع أي نوع بيانات	مصمم لحفظ سلاسل بيانات متسلسلة وثابتة

شفافية	غير شفاف، البيانات مشفرة ومخفاة	شفاف، يمكن للجميع رؤية السجل لكن لا يمكن تغييره
التعديل	يمكن تعديل البيانات إذا كان لديك المفتاح	لا يمكن تعديل البيانات بعد تسجيلها في البلوكشين

بدائل الحاسوب الكمي

المعيار	استخدام كروت شاشة لعمل حاسوب كمي	دمج التعدين مع الألعاب المكركة (غير قانوني)
التكلفة	تكلفة 1432 كرت شاشة 2.5 = مليون دولار	تكلفة حاسوب كمي من 15 = IBM مليون دولار
المكونات	يعتمد على كروت الشاشة المتطورة (GPU) لبناء الحاسوب الكمي	يعتمد على كروت الشاشة و ألعاب مكركة
القانونية	قانوني إذا تم استخدام الكروت في بناء حاسوب كمي	غير قانوني بسبب استخدام ألعاب مكركة
الأداء	أداء عالٍ في حل مسائل الكم والتوازي الحسابي	أداء متدهور بسبب التداخل بين التعدين والألعاب
الاستخدامات	الحوسبة الكمية مثل حل المشكلات المعقدة، المحاكاة، والأبحاث	التعدين أثناء لعب ألعاب مكركة (غير قانوني)
التأثير على الأجهزة	يمكن أن يؤثر على عمر الأجهزة بسبب العمليات الكمية المكثفة	تآكل أسرع للأجهزة بسبب التعدين المستمر والألعاب المكركة
المخاطر الأمنية	مخاطر قليلة إذا تم استخدام الأجهزة بطريقة آمنة	مخاطر أمنية كبيرة بسبب البرمجيات الضارة في الألعاب المكركة
العمر الافتراضي للأجهزة	قابل للتآكل بسبب الضغط المستمر من العمليات الكمية	ينخفض بشكل أسرع بسبب التعدين والألعاب المكركة
الاستدامة	مستدام مع التطور المستمر في الحوسبة الكمية	غير مستدام بسبب الاستخدام غير القانوني والأثر السلبي على الأجهزة