UOW

BLOCKCHAIN-BASED TEXT ENCRYPTION SYSTEM

نظام تشفير النصوص المبني على تقنية البلوكشين

BY SATTAR JABBAR & MAHMOUD SHAMRAN

SUPERVISION ASST. PROF. DR. ESRAA SALEH ALOMARIY

Blockchain Concept | مفهوم البلوكشين

- Chain of interconnected blocks
- Each block contains: index, timestamp, data, own hash, previous block hash
- Decentralized system distributed across multiple nodes
- Consensus principle between nodes for transaction verification

- سلسلة كتل مترابطة ببعضها البعض
- كل كتلة تحتوي على: فهرس، طابع زمني، بيانات، هاش خاص، وهاش للكتلة السابقة
- نظام لامركزي موزع بين عدة عقد
- مبدأ الإجماع بين العقد للتحقق من المعاملات

UOW

مفهوم الهاش في البلوكشين | Hashing Concept in Blockchain

Converting data to fixed-length string

Hash properties:

- Small changes produce completely different hashes
- Cannot reverse to retrieve original data
- Difficult to find two inputs with same hash

تحويل البيانات إلى سلسلة ثابتة الطول

خصائص الهاش:

- أي تغيير بسيط ينتج هاش مختلف تماماً
- لا يمكن عكس العملية لاسترجاع البيانات الأصلية
- صعوبة إيجاد محتويين مختلفين لهما نفس الهاش

UOW

آلية عمل البلوكشين في الأمن السيبراني | Blockchain in Cybersecurity

- Decentralization and distributed ledgers prevent single points of failure
- Cryptographic hash functions ensure data integrity
- Digital signatures for identity verification
- Consensus algorithms to ensure transaction validity

- اللامركزية والسجلات الموزعة تمنع نقاط الفشل المفردة
- دوال التجزئة التشفيرية لضمان سلامة البيانات
- التوقيعات الرقمية للتحقق من الهوية
- خوارزميات التوافق لضمان صحة المعاملات

UOW

مبادئ الحوسبة الكمية |
Quantum Computing Principles

- Using quantum properties like superposition and entanglement
- Qubit as basic information unit instead of traditional bit
- Ability to process vast amounts of data in parallel
- Capability to solve complex problems more efficiently

- استخدام الخصائص الكمية مثل التراكب والتشابك
- الكيوبت كوحدة معلومات أساسية بدلاً من البت التقليدي
- القدرة على معالجة كميات هائلة من البيانات بشكل متوازٍ
- إمكانية حل مشكلات معقدة بكفاءة أعلى

UOW

كيفية كسر أنظمة التشفير بواسطة الحوسبة الكمية | Quantum Computing Threats to Cybersecurity

- Shor's Algorithm: Direct threat to RSA and public key systems
- Grover's Algorithm: Accelerating database search and impact on symmetric encryption
- Attacks on quantum key distribution: Exploiting physical hardware flaws

- خوارزمية شور: تهديد مباشر لتشفير RSA وأنظمة المفتاح العام
- خوارزمية جروفر: تسريع البحث في قواعد البيانات وتأثيرها على التشفير المتماثل
- هجمات على توزيع المفاتيح الكمية: استغلال عيوب في الأجهزة الفيزيائية

UOW

Thank You