

BLOCKCHAIN-BASED TEXT ENCRYPTION SYSTEM

نظام تشفير النصوص المبني على تقنية البلوكشين

BY SATTARJABBAR&MAHMOUDSHAMRAN

SUPERVISION ASST.PROF.DR.ESRAASALEHALOMARIY



- Modern technology revolution and its impact on cybersecurity
- Importance of understanding these technologies against increasing threats
- How these technologies change the nature of cyber defense and attack
- Need for integration between different protection methods

- ثورة التقنيات الحديثة وتأثيرها على عالم الأمن السيبراني
- أهمية فهم هذه التقنيات في مواجهة التهديدات المتزايدة
- كيف تغير هذه التقنيات من طبيعة الدفاع والهجوم الإلكتروني
- الحاجة إلى التكامل بين الأساليب المختلفة للحماية الشاملة



- **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 متراكبة ببعضها البعض
- كل كتلة تحتوي على: فهرس، طابع زمني، بيانات، هاش خاص، وهاش للكتلة السابقة
- نظام لا مركزي موزع بين عدة عقد
- مبدأ الإجماع بين العقد للتحقق من المعاملات

- Decentralization and distributed ledgers prevents 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

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

دور العقد في شبكة البلوكشين | Blockchain Security and Distributed Nodes

- Each node maintains complete copy of blockchain
- Ensures data integrity and prevents tampering
- System continuity even if some nodes fail
- Network consensus on data validity

- كل عقدة تحتفظ بنسخة كاملة من سلسلة الكتل
- تأمين التحقق من عدم التلاعب بالبيانات
- استمرارية النظام حتى عند تعطل بعض العقد
- إجماع الشبكة على صحة البيانات



آكيفية كسر أنظمة البلوكشين | Blockchain Security Challenges

- 1. 51% attack: Controlling more than half of computing power**
- 2. Attacks on digital signatures: Exploiting weakness in random number generation**
- 3. Sybil attacks: Creating multiple fake identities**
- 4. Smart contract vulnerabilities: Exploiting programming errors**



- 1. هجوم الـ51%: السيطرة على أكثر من نصف قوة الحوسبة**
- 2. هجمات على التوقيعات الرقمية: استغلال ضعف في توليد الأرقام العشوائية**
- 3. هجمات Sybil: إنشاء هويات متعددة مزيفة**
- 4. الثغرات في العقود الذكية: استغلال أخطاء البرمجة**

- 1. Split text into chunks**
- 2. Generate proof-of-work for new block**
- 3. Derive key from proof**
- 4. Encrypt chunk using appropriate algorithm**
- 5. Store encrypted chunk and key in new block**

١. تقسيم النص إلى أجزاء

٢. توليد إثبات العمل للكتلة الجديدة

٣. استخراج مفتاح من الإثبات

٤. تشفير الجزء باستخدام خوارزمية مناسبة

٥. تخزين الجزء المشفر والمفتاح في كتلة جديدة



- 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

- **Quantum Key Distribution (QKD) for secure key exchange**
- **Post-quantum cryptography to counter quantum computer capabilities**
- **Development of new algorithms based on mathematical problems difficult even for quantum computers**



- توزيع المفاتيح الكمية (QKD) للتبادل الآمن للمفاتيح
- التشفير المقاوم لكم لمواجهة قدرات الحواسيب الكمية
- تطوير خوارزميات جديدة تعتمد على مشاكل رياضية صعبة حتى للحواسيب الكمية

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 لـ RSA وأنظمة المفتاح العام
- خوارزمية جروف: تسريع البحث في قواعد البيانات وتأثيرها على التشفير المتماثل
- هجمات على توزيع المفاتيح الكمية: استغلال عيوب في الأجهزة الفيزيائية

كيف يمكن دمج هذه التقنيات لتعزيز الأمان السيبراني | Integration Between the Three Technologies Cybersecurity

AI with Blockchain:

- Transaction analysis and suspicious pattern detection
- Documenting AI models on blockchain

AI with Quantum Computing:

- Improving quantum encryption protocols
- Developing models resistant to quantum attacks

Blockchain with Quantum Computing:

- Quantum-resistant blockchain protocols
- Securing blockchain transactions using quantum key distribution

الذكاء الاصطناعي مع البلوكشين:

- تحليل المعاملات واكتشاف الأنماط المشبوهة
- توثيق نماذج الذكاء الاصطناعي على البلوكشين

الذكاء الاصطناعي مع الحوسبة الكمية:

- تحسين بروتوكولات التشفير الكمي
- تطوير نماذج مقاومة للهجمات الكمية
- البلوكشين مع الحوسبة الكمية:

- بروتوكولات بلوكشين مقاومة لكم تأمين معاملات البلوكشين باستخدام توزيع المفاتيح الكمية



تطبيق عملي - نظام تشفير النصوص | Practical Application - Text Encryption System

- **Practical Application - Text Encryption System:** Backend: Python with Flask framework
- Frontend: HTML, CSS, JavaScript
- Encryption: Advanced algorithms with blockchain integration
- Animations: Visual effects to explain the process
- User Interface: Tabs for encryption, decryption, attack simulation
- Blockchain and node status display
- Visual representation of encryption process and block linking

- مكونات النظام: الواجهة الخلفية: بايثون مع إطار عمل Flask
- الواجهة الأمامية: HTML, CSS, JavaScript
- التشفير: خوارزميات متقدمة مع دمج البلوكشين
- الرسوم المتحركة: تأثيرات مرئية لتوضيح العملية
- واجهة المستخدم: تبويبات للتشفير، فك التشفير، محاكاة الهجمات
- عرض حالة البلوكشين والعقد
- تمثيل مرئي لعملية التشفير وربط الكتل



نظام التشفير بالبلوكشين

نظام التشفير بالبلوكشين

حالات العمل:

- فك التشفير:** حالات العمل المنشورة هنا هي الحالات التي تم فك تشفيرها بنجاح.
- كسر التشفير:** حالات العمل المنشورة هنا هي الحالات التي تم كسر تشفيرها بنجاح.
- حالة البلوكشين:** حالات العمل المنشورة هنا هي الحالات التي تم إنشاؤها في نظام البلوكشين.

النافذة الرئيسية:

فك تشفير النص:

النص الأصلي: محمود

النص المشفر: م

الكلمات المفتاحية: a8d855c9b492a683, cc6a251fac8cad5d, a59993450b045e08, 3ab62bff400de677, b99da1d10097a860

محاكاة كسر التشفير:

الكلمات المفتاحية: a8d855c9b492a683, cc6a251fac8cad5d, a59993450b045e08, 3ab62bff400de677, b99da1d10097a860

نتيجة كسر التشفير:

النص المشفر	الكلمات المفتاحية	النص الأصلي
م	a8d855c9b492a683	م
ـ	cc6a251fac8cad5d	ـ
ـ	a59993450b045e08	ـ
ـ	3ab62bff400de677	ـ
ـ	b99da1d10097a860	ـ

نظام التشفير بالبلوكشين

نظام التشفير بالبلوكشين

حالات العمل:

- فك التشفير:** حالات العمل المنشورة هنا هي الحالات التي تم فك تشفيرها بنجاح.
- كسر التشفير:** حالات العمل المنشورة هنا هي الحالات التي تم كسر تشفيرها بنجاح.
- حالة البلوكشين:** حالات العمل المنشورة هنا هي الحالات التي تم إنشاؤها في نظام البلوكشين.

النافذة الرئيسية:

تشفيـر النـص باـسـتـخـادـ الـبـلـوـكـشـين:

النص الأصلي: محمود

النص المشفر: م

الكلمات المفتاحية: a8d855c9b492a683, cc6a251fac8cad5d, a59993450b045e08, 3ab62bff400de677, b99da1d10097a860

نتـجـةـ التـشـفـير:

النص المشفر	الكلمات المفتاحية	النـصـ الأـصـلـي
م	a8d855c9b492a683	م
ـ	cc6a251fac8cad5d	ـ
ـ	a59993450b045e08	ـ
ـ	3ab62bff400de677	ـ
ـ	b99da1d10097a860	ـ

الـجـانـبـ الـعـمـلـيـ -ـ التـنـفـيـذـ

Page 14 of 17

- **Blockchain linking using hash references**
- **Visual encryption with node simulation**
- **Decentralization and distribution concepts**
- **AI integration for breach detection**
- **Applying quantum computing principles for enhanced security**

- ربط كتل البلوكشين باستخدام روابط الهاش
- التشفير المرئي مع محاكاة العقد
- مفهوم اللامركبية والتوزيع
- تكامل الذكاء الاصطناعي للكشف عن محاولات الاختراق
- تطبيق مبادئ الحوسبة الكمية لتعزيز الأمان



- Advanced consensus mechanisms (PoS, PBFT)
- Transport layer encryption with TLS/SSL
- Public/private key encryption
- Network monitoring using AI
- Implementing quantum-resistant algorithms

- آليات إجماع متقدمة (Proof of Stake, PBFT)
- تشفير طبقة النقل باستخدام TLS/SSL
- تشفير المفاتيح العامة/الخاصة
- مراقبة الشبكة باستخدام الذكاء الاصطناعي
- تطبيق خوارزميات مقاومة للحوسبة الكمية



Thank You

