SHA-256 Hashing in Trade Finance Systems

1. What is Hashing?

Hashing is a one-way mathematical process that converts any input data into a fixed-length output called a hash. It is used to ensure data integrity and tamper detection, not confidentiality.

2. Hashing vs Encryption

Hashing is irreversible and used for integrity verification, while encryption is reversible and used for data confidentiality.

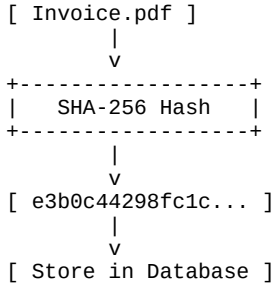
3. What is SHA-256?

SHA-256 stands for Secure Hash Algorithm (256-bit). It produces a 256-bit (64 hexadecimal characters) output regardless of input size.

4. Key Properties of SHA-256

Deterministic, fixed-length, one-way (pre-image resistant), collision resistant, and avalanche effect.

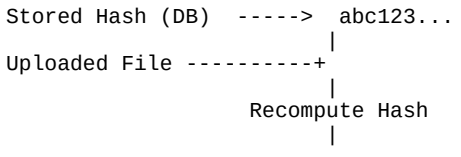
Whiteboard Diagram 1: Document Hashing Flow



5. Why Hashing is Critical in Trade Finance

Trade finance documents are legal and financial artifacts. Hashing ensures that any post-upload modification is detected instantly.

Whiteboard Diagram 2: Verification Process



```
                    Match ?  YES / NO
```

6. Case Study 1: Invoice Tampering Detection

A corporate uploads an invoice for $100,000. The system stores its SHA-256 hash. Later, the invoice amount is modified to $900,000. On verification, the recomputed hash does not match the stored hash, immediately detecting fraud.

7. Case Study 2: Auditor Verification

An auditor downloads a Bill of Lading and independently computes its hash. They compare it with the hash stored in the ledger. Matching hashes prove the document was never altered since submission.

8. Hashing and Ledger Integrity

Each ledger entry references document hashes, creating an immutable audit trail. Any attempt to alter historical data breaks the hash chain and is detected.

Whiteboard Diagram 3: Ledger Chain Concept

```
[ Entry 1 ]
 Hash: H1
   |
[ Entry 2 ]
 Hash: H2 (includes H1)
   |
[ Entry 3 ]
 Hash: H3 (includes H2)
```

9. Compliance and Regulatory Importance

Regulators require proof that documents were not altered. SHA-256 provides mathematical evidence of integrity.

10. Summary

SHA-256 hashing acts as a digital fingerprint for trade finance documents, enabling tamper detection, audit trust, and compliance-grade integrity verification.