L02: Cryptographic Foundations

BSc Blockchain Course

Digital Finance

2026

Learning Objectives

By the end of this lesson, you will be able to:

1. Explain the properties of cryptographic hash functions
2. Describe how digital signatures provide authentication
3. Understand elliptic curve cryptography basics (ECDSA)
4. Explain how Merkle trees enable efficient verification
5. Derive a blockchain address from a public key

These primitives are the foundation of all blockchain security.

Cryptographic Hash Functions

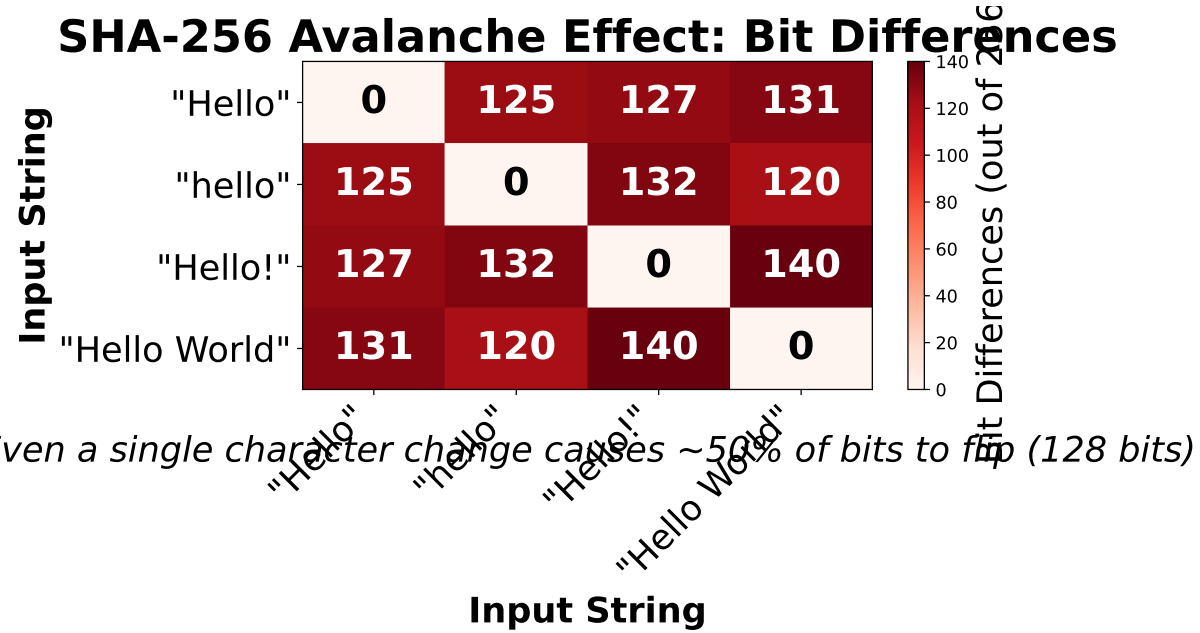
Four Key Properties

- Deterministic: Same input always yields same output
- One-way: Cannot reverse to find input
- Collision resistant: Hard to find two inputs with same output


```
Example: SHA-256("Hello") = 185f8db32271fe25f561a...
```

SHA-256 (Bitcoin) and Keccak-256 (Ethereum) are the primary hash functions.

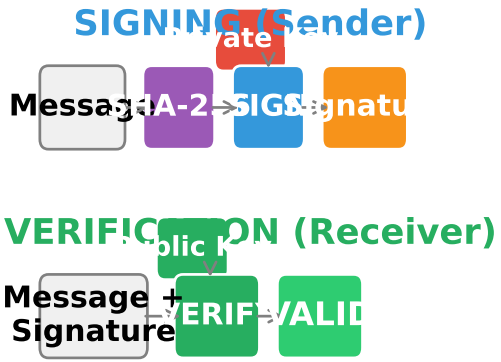
Avalanche Effect



Even a single character change causes ~50% of bits to flip (128 bits)

A single bit change causes approximately 50% of output bits to flip.

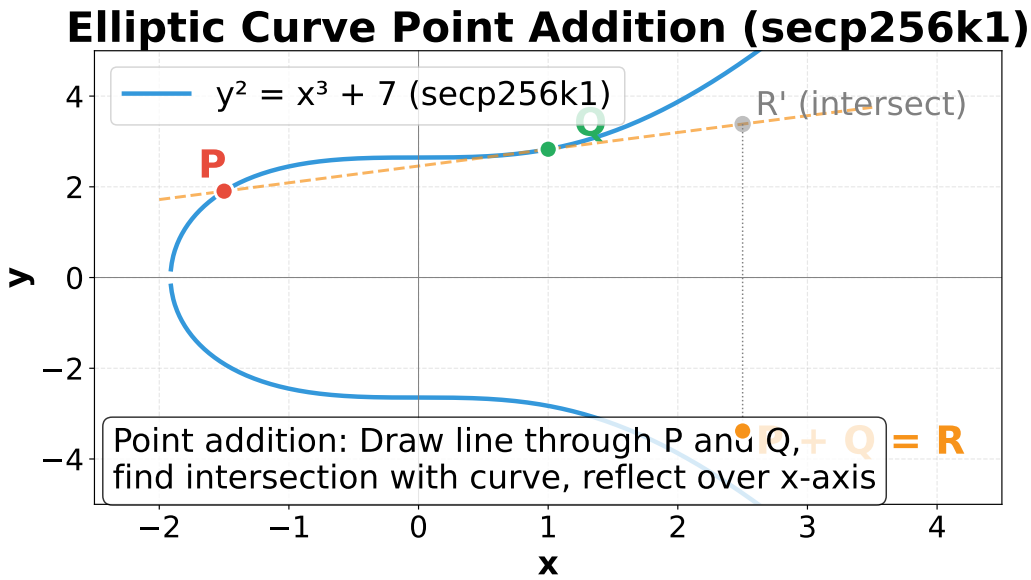
Digital Signatures



Private key signs, public key verifies. Only the owner can sign, anyone can verify.

Private key signs; public key verifies. Only owner can sign.

Elliptic Curve Cryptography



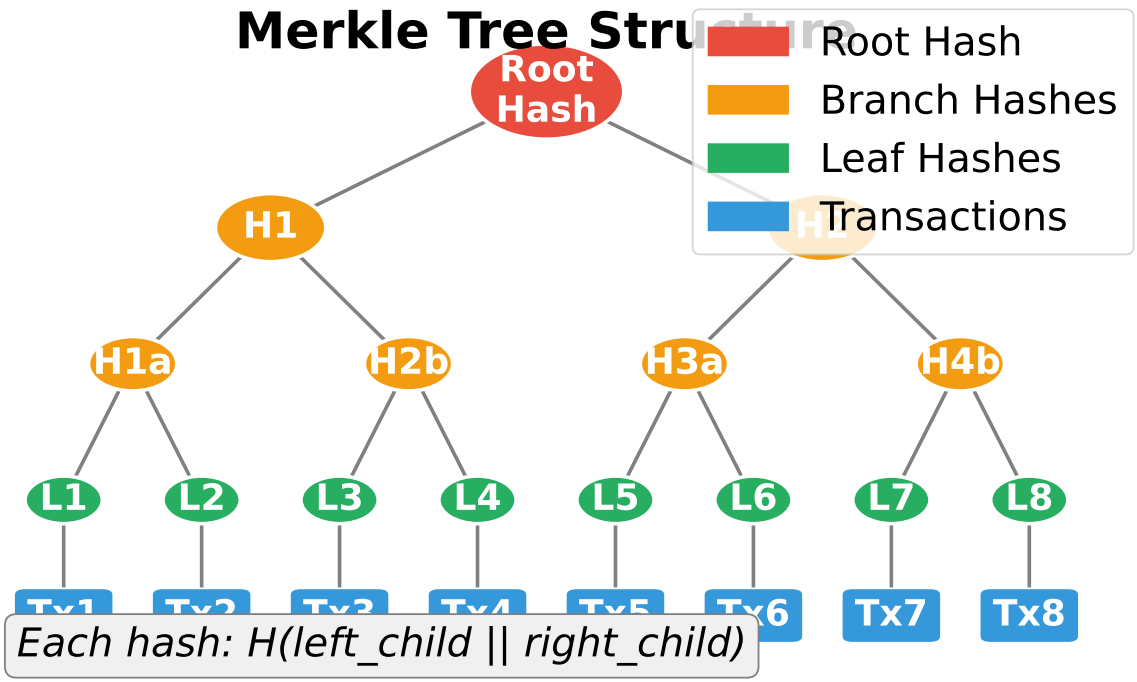
secp256k1 curve used by Bitcoin and Ethereum. Point addition is the core operation.

Private key -> Public key (easy) | Public key -> Private key (impossible)

Key Generation Process

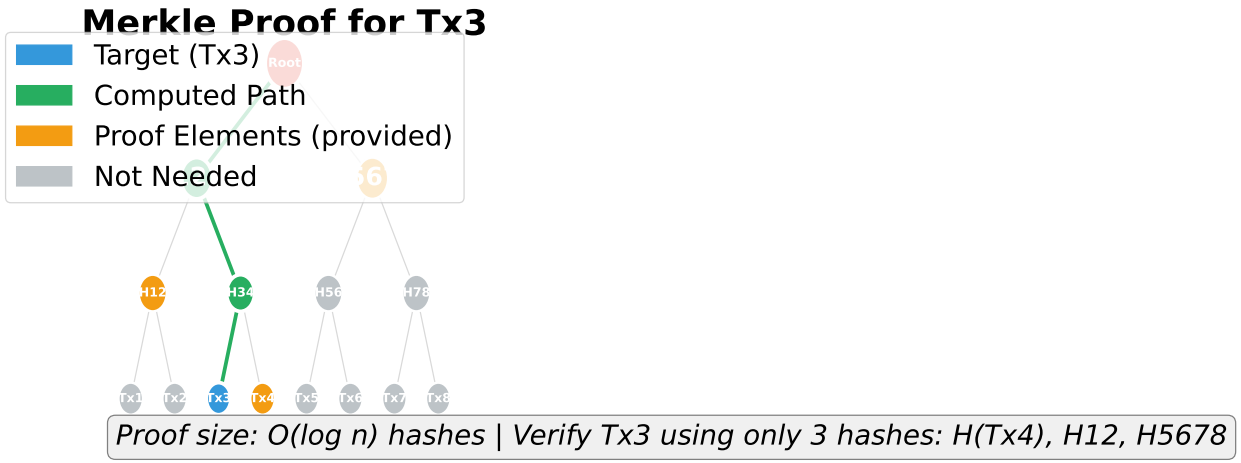
Private key to public key is easy; reverse is computationally infeasible.

Merkle Trees



Binary hash tree enables O(log n) transaction verification.

Merkle Proofs



Light clients can verify transactions without downloading entire blocks.

Key Takeaways

Remember These Points

1. Hash functions provide integrity and link blocks together
2. Digital signatures prove ownership without revealing private keys
3. ECDSA enables compact signatures (64 bytes vs RSA 256+)
4. Merkle trees allow efficient verification in O(log n)
5. Addresses are derived from public keys via hashing

Next Lesson: Bitcoin Deep Dive – UTXO model, mining, and transaction structure.