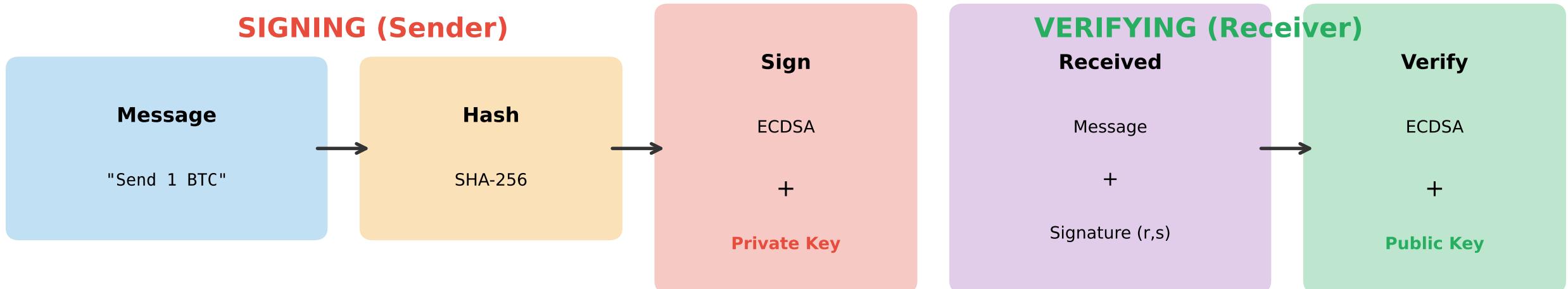


Digital Signature: Sign and Verify



Digital Signature Properties

Authentication: Only private key holder can create valid signature

Integrity: Any change to message invalidates signature

Non-repudiation: Signer cannot deny having signed

In Bitcoin Transactions:

Sender signs transaction with private key

Network verifies using sender's public key (from address)

Proves ownership of funds without revealing private key