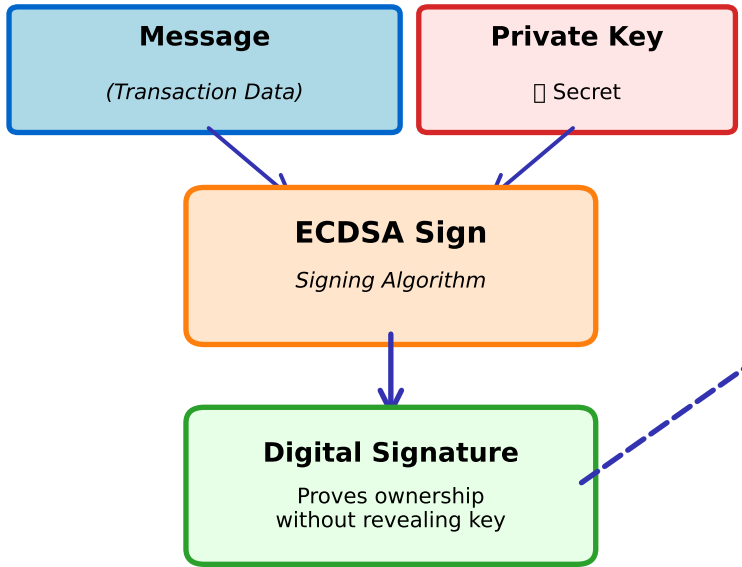


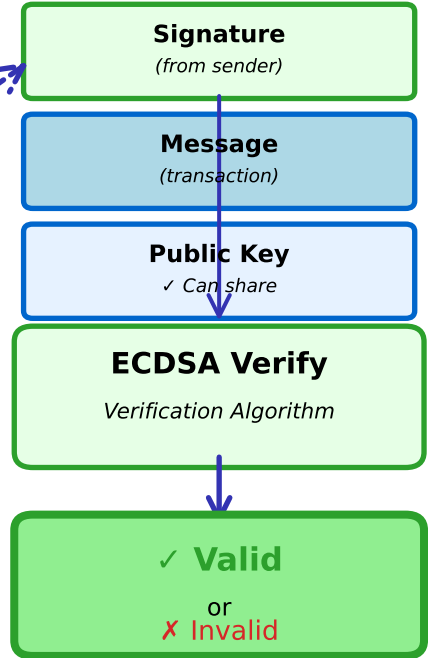
# Digital Signature Flow

How Bitcoin transactions are signed and verified

## SIGNING



## VERIFICATION



Broadcast to network

- Key Properties:
- Only private key holder can create valid signature
    - Anyone with public key can verify signature
  - Signature is unique to both message and private key
    - Tampering with message invalidates signature