ECDSA: Elliptic Curve Digital Signature Algorithm

SIGNING

1. Hash message

```
z = SHA256(message)
```

2. Random k

```
k = random [1, n-1]
```

3. Calculate R

```
R = k*G, r = R.x mod n
```

4. Calculate s

```
s = k^-1(z + r*d) mod n
```

5. Signature

```
sig = (r, s)
```

VERIFICATION

1. Hash message

```
z = SHA256(message)
```

2. Calculate u1

```
u1 = z * s^-1 mod n
```

3. Calculate u2

```
u2 = r * s^-1 mod n
```

4. Calculate P

```
P = u1*G + u2*Q
```

5. Check

```
Valid if P.x mod n = r
```

Variables: G=generator, n=curve order, d=private key, Q=public key, k=nonce

Bitcoin uses secp256k1 curve with 256-bit keys and SHA-256 hashing

Source: SEC 1: Elliptic Curve Cryptography, ANSI X9.62