

Bitcoin Address Derivation: From Private Key to Address

Cannot reverse: Address -> Private Key

One-way function

Private Key

256-bit random
number

256 bits
(secret!)

Public Key

$Q = k * G$
(x, y coordinates)

33 or 65 bytes
(public)

Hash

SHA-256 +
RIPEMD-160

20 bytes
(160 bits)

Checksum

Double SHA-256
(first 4 bytes)

4 bytes

Address

Base58
encoded

25-34 chars
1A1zP1...