

?, ?, ?, ?

A very simple and a very short but a very powerful program:

```
Ⓜ  
  
show (Ⓜ);  
show (Ⓜ);  
  
show Ⓜalso Ⓜ  
  
save as blox;
```

Output

"Ⓜ" → "0x40d93f50D4a56Be60fDe352c01097E1E42405b69"

"Ⓜ" → "0xa020807ff2c90743afbc8c5f74c191cb6eb037f1613211d42a4bf3977e5f9f0"

"Ⓜ" → <|"Type" -> "EllipticCurve", "CurveName" -> "secp256k1", "Compressed" -> False,

"PublicKey" -> {4, 250, 117, 78, 63, 249, 35, 37, 119, 220, 59, 73, 128, 250, 4, 178, 253, 14,  
126, 0, 19, 129, 44, 182, 137, 197, 161, 110, 203, 53, 24, 120, 64, 179, 9, 240, 194, 86, 37, 144,  
38, 84, 88, 224, 184, 173, 242, 231, 142, 52, 104, 62, 26, 166, 48, 141, 145, 95, 228, 62, 101, 132,  
235, 155, 110},

"PublicCurvePoint" ->

{11328547331332457675378811984661559764481072006219424404727484241178193248057  
6,  
80981563178412881780651944120220270359429660115039823663624727923423640787822}

|>

"Ⓜ" → <|"Type" -> "EllipticCurve", "CurveName" -> "secp256k1",

"PublicCurvePoint" ->

{11328547331332457675378811984661559764481072006219424404727484241178193248057  
6,  
80981563178412881780651944120220270359429660115039823663624727923423640787822},

"PrivateMultiplier" ->

72427481752409419219811996059199421334290305641324603076644566044143119628784,

"Compressed" -> False,

"PublicByteArray" -> {4, 250, 117, 78, 63, 249, 35, 37, 119, 220, 59, 73, 128, 250, 4, 178, 253, 14, 126, 0, 19, 129, 44, 182, 137, 197, 161, 110, 203, 53, 24, 120, 64, 179, 9, 240, 194, 86, 37, 144, 38, 84, 88, 224, 184, 173, 242, 231, 142, 52, 104, 62, 26, 166, 48, 141, 145, 95, 228, 62, 101, 132, 235, 155, 110},

"PrivateByteArray" -> {160, 32, 128, 127, 242, 201, 7, 67, 175, 188, 184, 197, 247, 76, 25, 28, 182, 235, 3, 127, 22, 19, 33, 29, 66, 164, 191, 57, 119, 229, 249, 240}

|>

---

Revision #11

Created 2026-05-18 03:13:08 UTC by Dara

Updated 2026-05-21 20:33:16 UTC by Dara