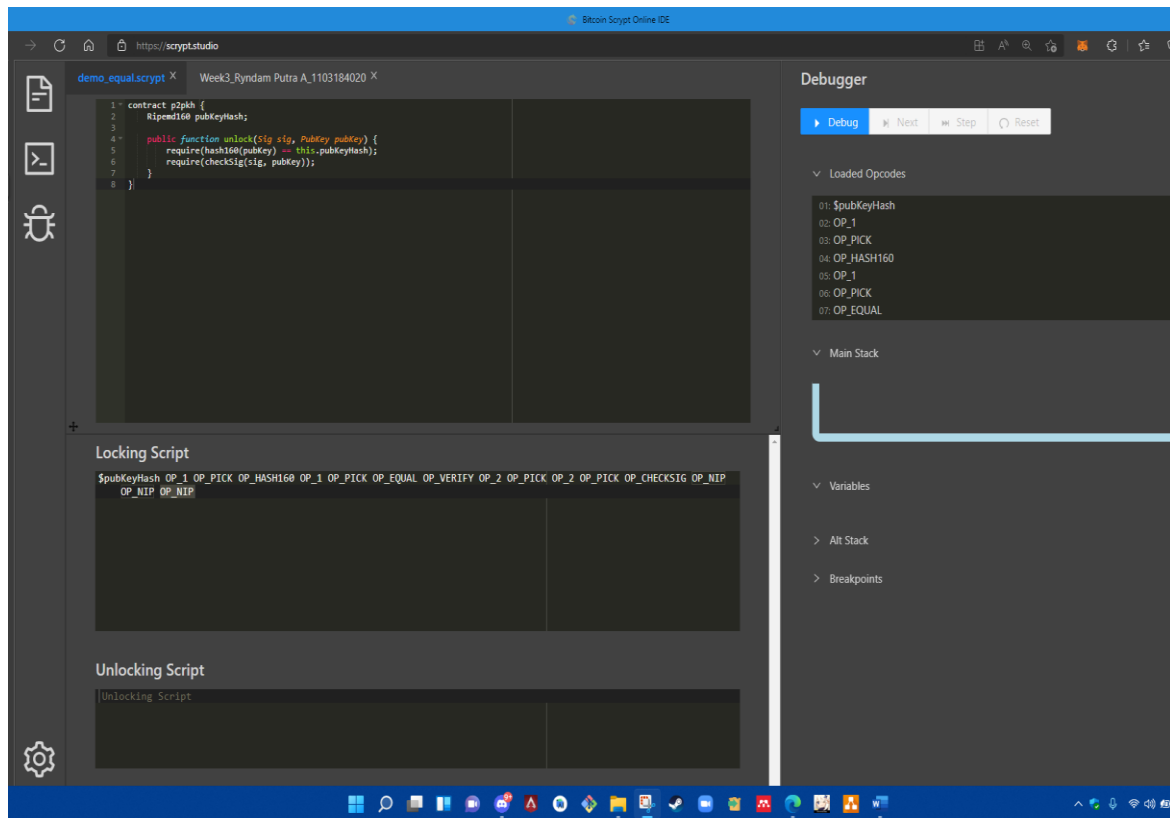


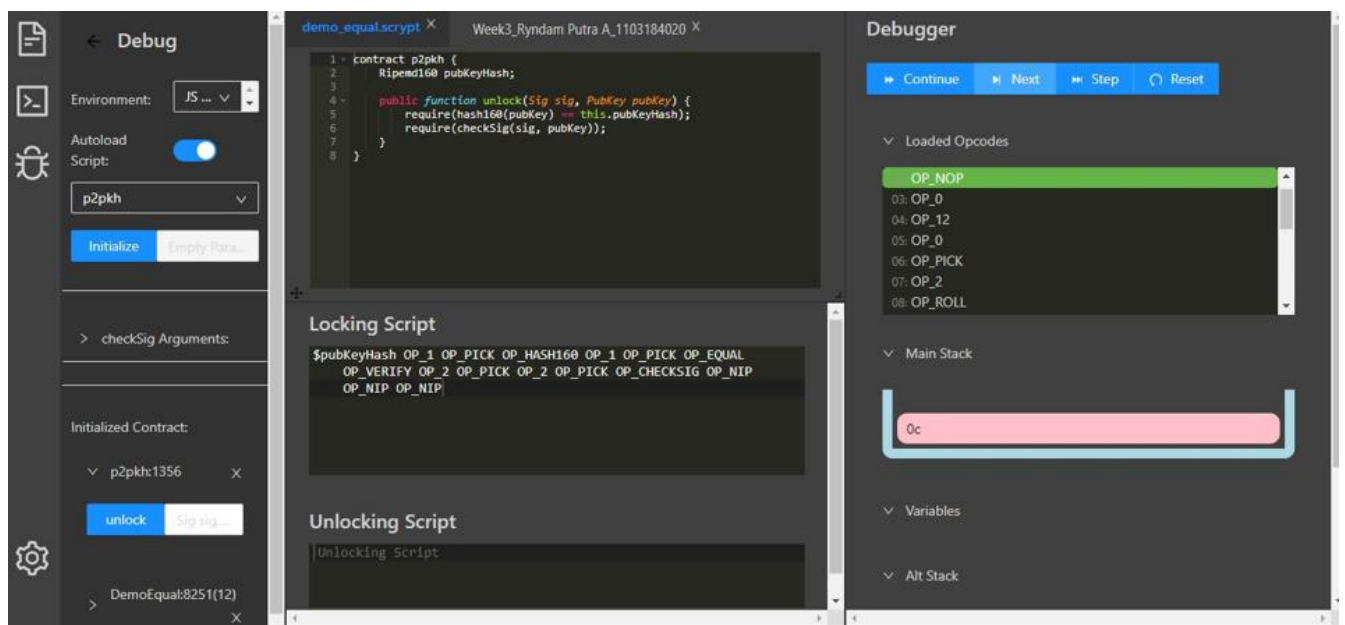
Nama : Ryndam Putra A

Nim : 1103184020

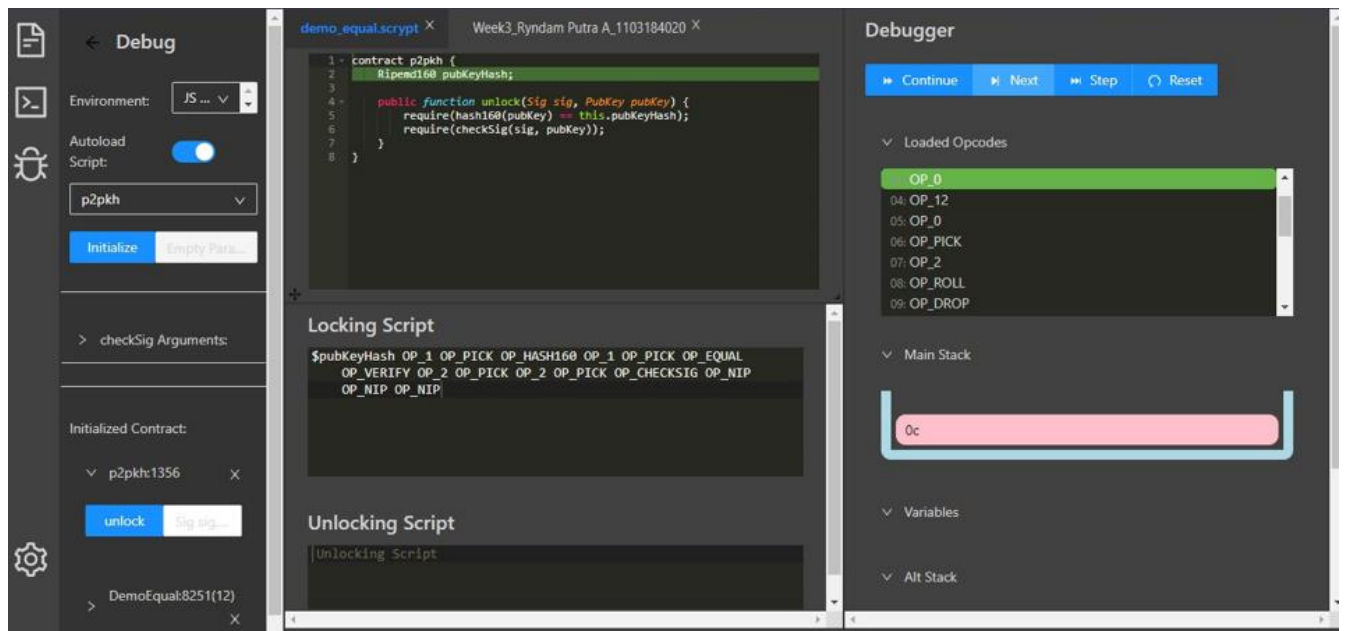


Dari ini kita mencoba code p2pkh yang dimana digunakan untuk mengirim bitcoin ke alamat bitcoin yang kontrak nya dibuka oleh kunci public dan tanda tangan dibuat oleh kunci pribadi yang sesuai.

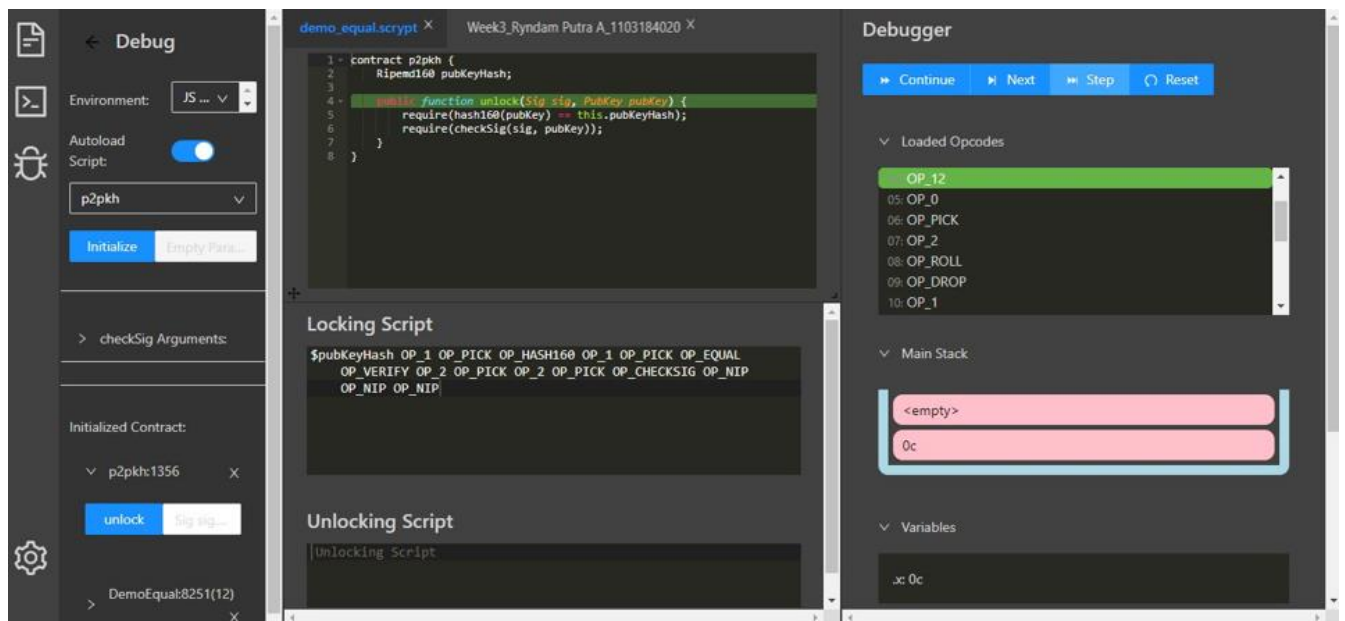
Nah didalam tampilan yang sudah ada locking script yang dimana berupa script-script tersebut lalu diloaded opcodes(di sebelah kanan) itu akan diproses di dalam bitcoin script virtual mechine ini.



Ketika kita klik next pada bawah debugger pada loaded opcode pada script (op_nop) akan diproses ke main stack dengan hasil 0c.



Lalu masuk ke ripedm160 pubkeyhash dan menuju ke script OP_0, terus di periksasetiap script nya sehingga menghasilkan seperti ini :



Debug

Environment: JS ...

Autoload Script: ☒

Script: p2pkh

Initialize Empty Para...

checkSig Arguments:

Initialized Contract:

p2pkh:1356

unlock Sig sig...

DemoEqual:8251(12)

demo_equal.script Week3_Ryndam Putra A_1103184020

```
1 contract p2pkh {
2   Ripemd160 pubKeyHash;
3
4   public function unlock(Sig sig, PubKey pubKey) {
5     require(hash160(pubKey) == this.pubKeyHash);
6     require(checkSig(sig, pubKey));
7   }
8 }
```

Locking Script

\$pubKeyHash OP_1 OP_PICK OP_HASH160 OP_1 OP_PICK OP_EQUAL
OP_VERIFY OP_2 OP_PICK OP_2 OP_PICK OP_CHECKSIG OP_NIP
OP_NIP OP_NIP

Unlocking Script

Unlocking Script

Debugger

Continue Next Step Reset

Loaded Opcodes

OP_0
06: OP_PICK
07: OP_2
08: OP_ROLL
09: OP_DROP
10: OP_1
11: OP_ROLL

Main Stack

0c
<empty>
0c

Variables

Debug

Environment: JS ...

Autoload Script: ☒

Script: p2pkh

Initialize Empty Para...

checkSig Arguments:

Initialized Contract:

p2pkh:1356

unlock Sig sig...

DemoEqual:8251(12)

demo_equal.script Week3_Ryndam Putra A_1103184020

```
1 contract p2pkh {
2   Ripemd160 pubKeyHash;
3
4   public function unlock(Sig sig, PubKey pubKey) {
5     require(hash160(pubKey) == this.pubKeyHash);
6     require(checkSig(sig, pubKey));
7   }
8 }
```

Locking Script

\$pubKeyHash OP_1 OP_PICK OP_HASH160 OP_1 OP_PICK OP_EQUAL
OP_VERIFY OP_2 OP_PICK OP_2 OP_PICK OP_CHECKSIG OP_NIP
OP_NIP OP_NIP

Unlocking Script

Unlocking Script

Debugger

Continue Next Step Reset

Loaded Opcodes


OP_1
15: OP_PICK
16: OP_1
17: OP_PICK
18: OP_NUMEQUAL
19: OP_NIP
20: OP_NIP

Main Stack


0c
0c

Variables


0c



Debug



Environment: JS ...



Autoload Script: ☒

p2pkh

Initialize Empty Para...

> checkSig Arguments:

Initialized Contract:

p2pkh1356

unlock Sig sig...

> DemoEquat8251(12)

demo_equalscript x Week3_Ryndam Putra A_1103184020 x

```
1 contract p2pkh {
2   Ripemd160 pubkeyHash;
3
4   public function unlock(Sig sig, PubKey pubkey) {
5     require(hash160(pubKey) == this.pubkeyHash);
6     require(checkSig(sig, pubkey));
7   }
8 }
```

Locking Script

\$pubkeyHash OP_1 OP_PICK OP_HASH160 OP_1 OP_PICK OP_EQUAL
OP_VERIFY OP_2 OP_PICK OP_2 OP_PICK OP_CHECKSIG OP_NIP
OP_NIP OP_NIP

Unlocking Script

Unlocking Script

Debugger

Debug Next Step Reset

Execution Successful

Loaded Opcodes

14: OP_1
15: OP_PICK
16: OP_1
17: OP_PICK
18: OP_NUMEQUAL
19: OP_NIP
20: OP_NIP

Main Stack

01

Variables