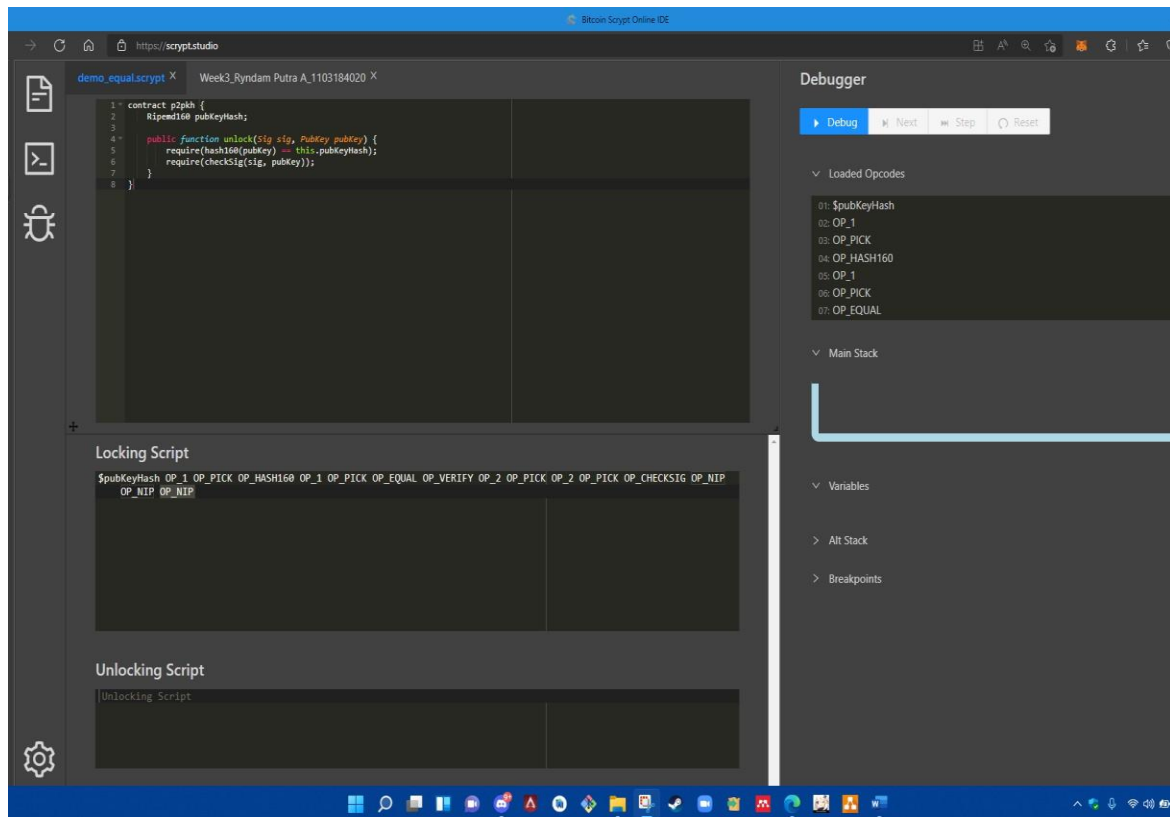


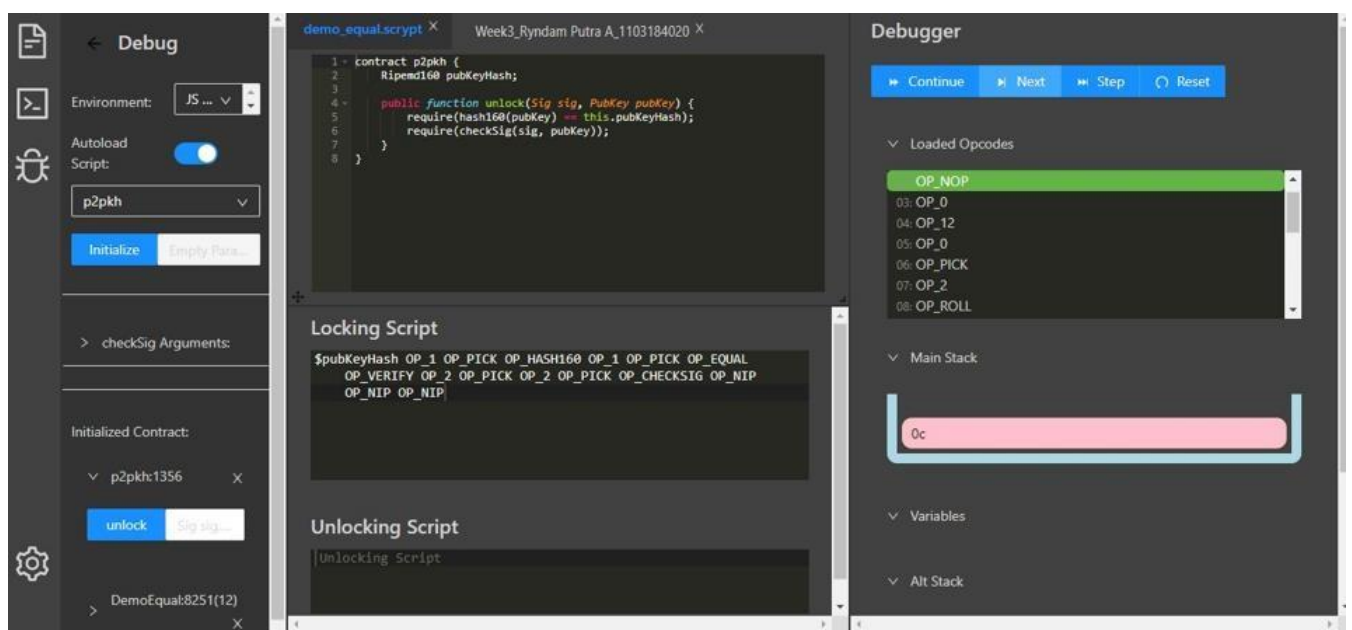
Sutan Faiz Rasyid

1103183160

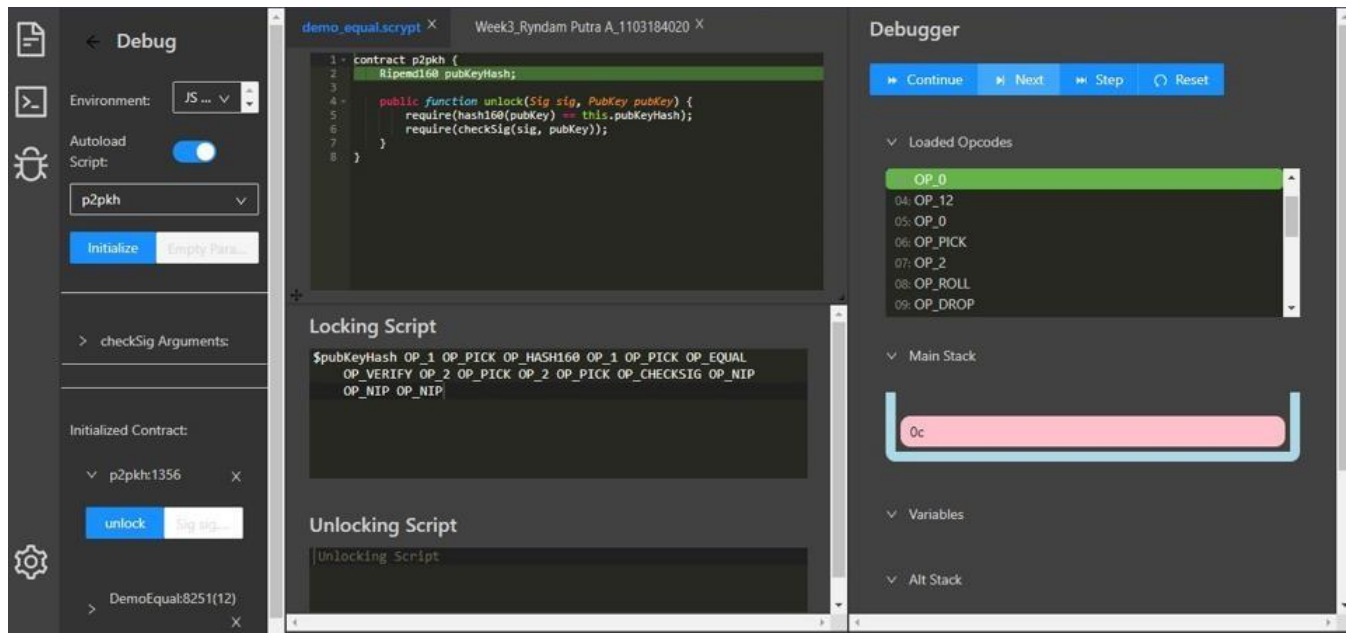


Dari ini kita mencoba code p2pkh yang dimana digunakan untuk mengirim bitcoin ke alamat bitcoin yang kontrak nya dibuka oleh kunci public dan tanda tangan dibuat oleh kunci pribadi yang sesuai.

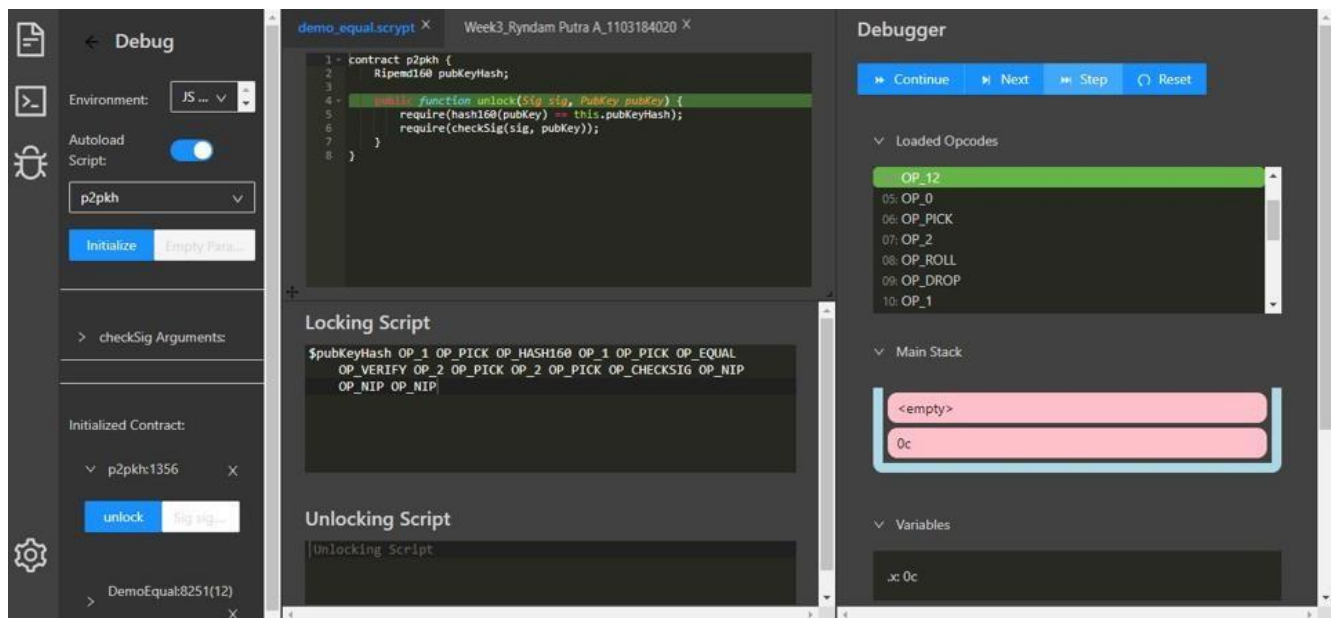
Nah didalam tampilan yang sudah ada locking script yang dimana berupa script-script tersebut lalu diloaded opcodes(di sebelah kanan ) itu akan diproses di dalam bitcoin script virtual mechine ini.



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 `ripemd160 pubkeyhash` dan menuju ke script `OP_0`, terus di periksa setiap script nya sehingga menghasilkan seperti ini :



Debug

Environment: JS ...

Autoload Script: ☒

p2pkh

Initialize Empty Para...

checkSig Arguments:

Initialized Contract:

p2pkh:1356

unlock Sig sig...

DemoEqual8251(12)

demo\_equal\_script Week3\_Rydam 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: ☒

p2pkh

Initialize Empty Para...

checkSig Arguments:

Initialized Contract:

p2pkh:1356

unlock Sig sig...

DemoEqual8251(12)

demo\_equal\_script Week3\_Rydam 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


.c: 0c



Debug



Environment: JS ...



Autoload 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

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