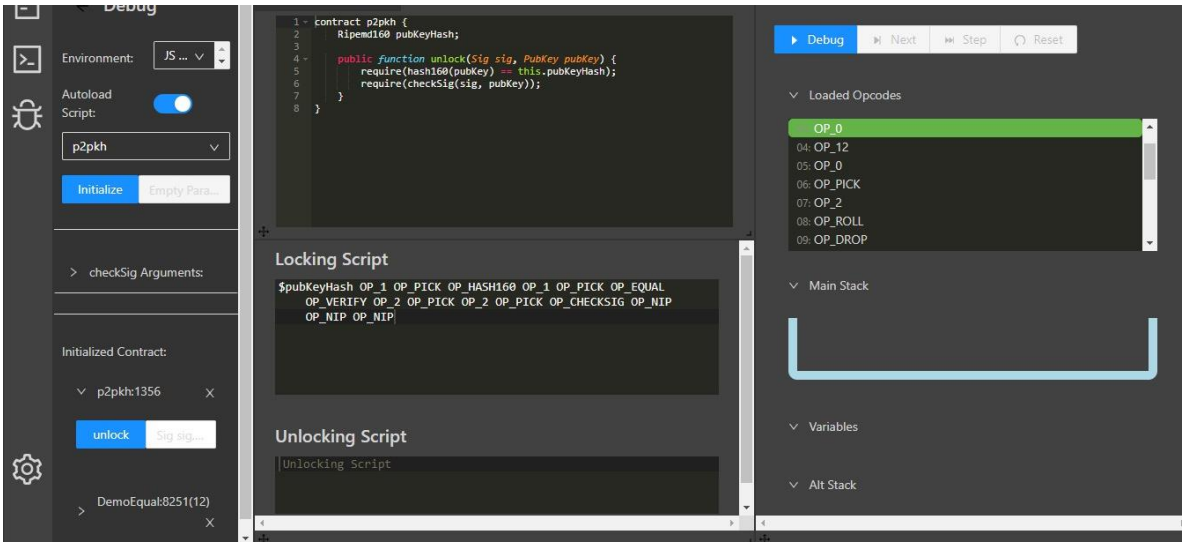
Nama : Raihan Puspa AP

NIM : 1103184065

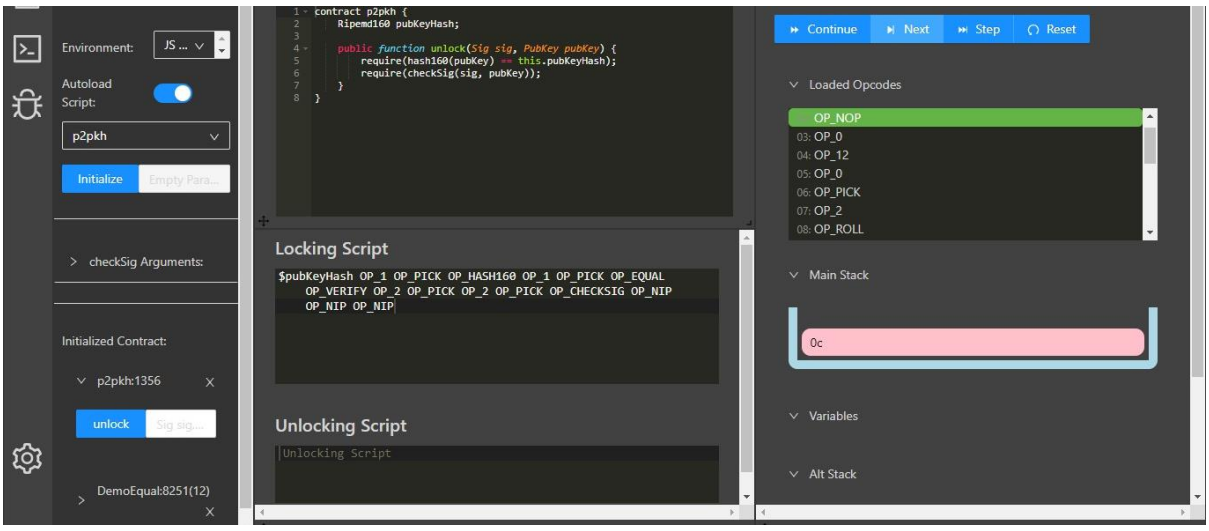
TUGAS WEEK 3

- Mencoba code yang digunakan untuk mengirim bitcoin ke alamat bitcoin yang kontraknya dibuka oleh key public dan tanda tangan dibuat oleh kunci pribadi yang sesuai.

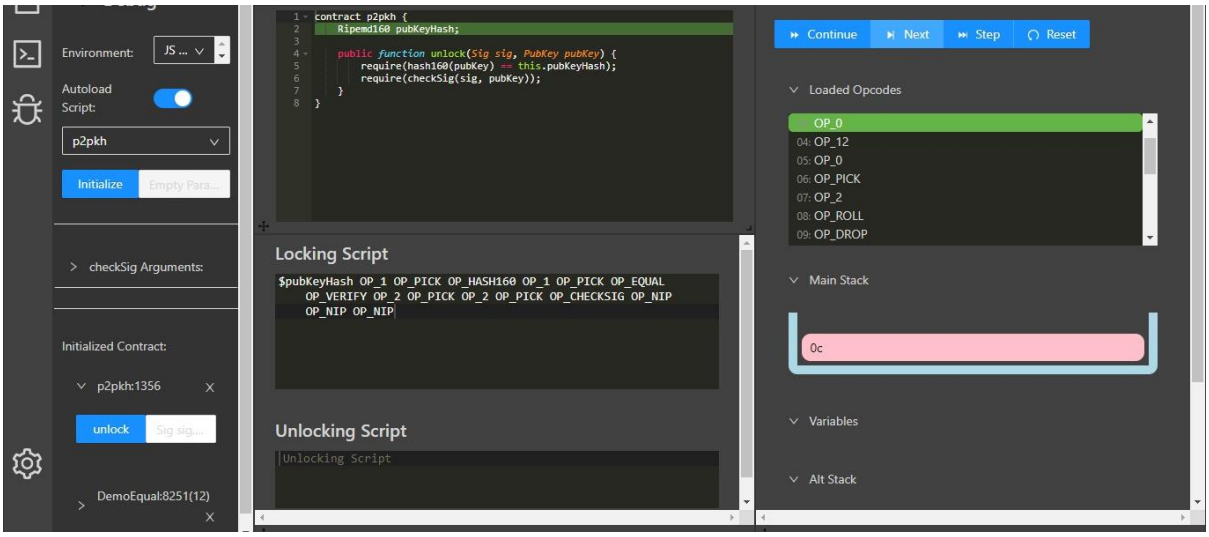


- Dalam tampilan sudah ada locking script yang dimana berupa script-script tersebut lalu diloaded opcodes(sebelah kanan) itu akan diproses di dalam bitcoin script virtual mechine ini.

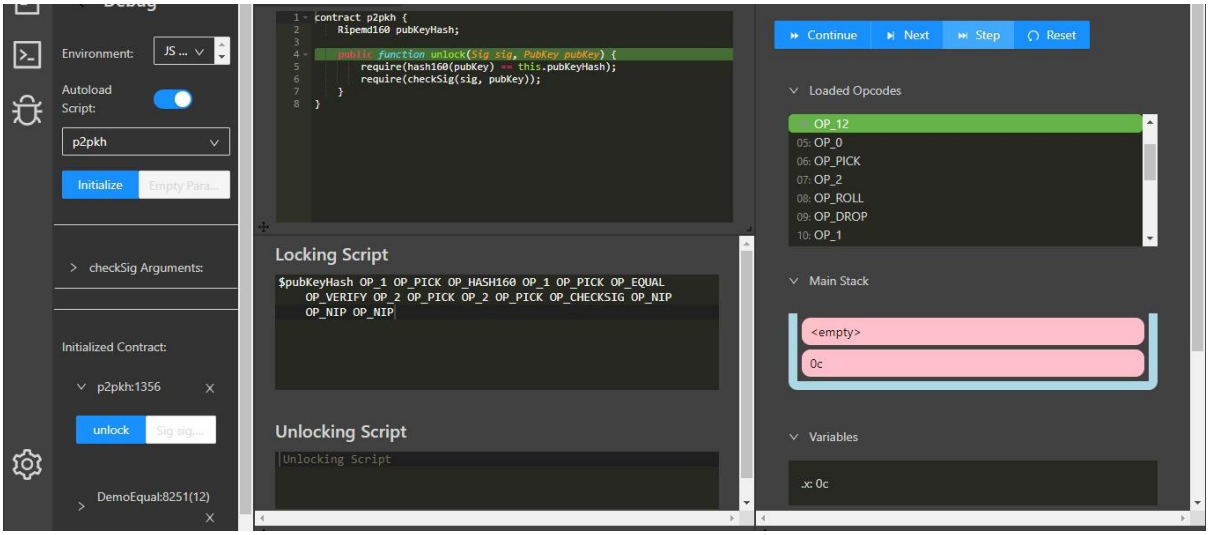
- Ketika kita klik next pada bawah debugger pada loaded opcode pada script (op_nop) akan di proses ke

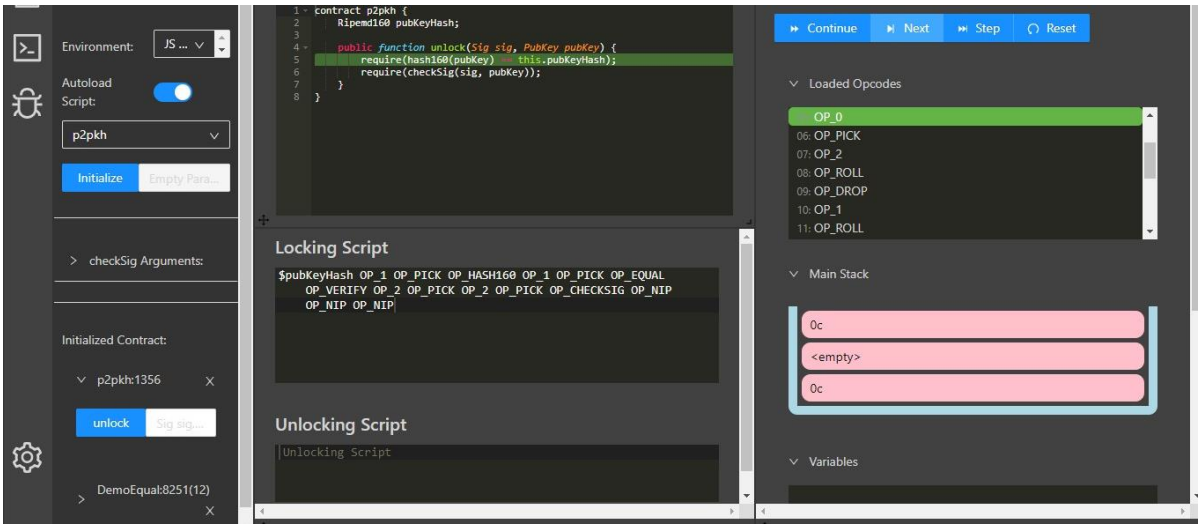


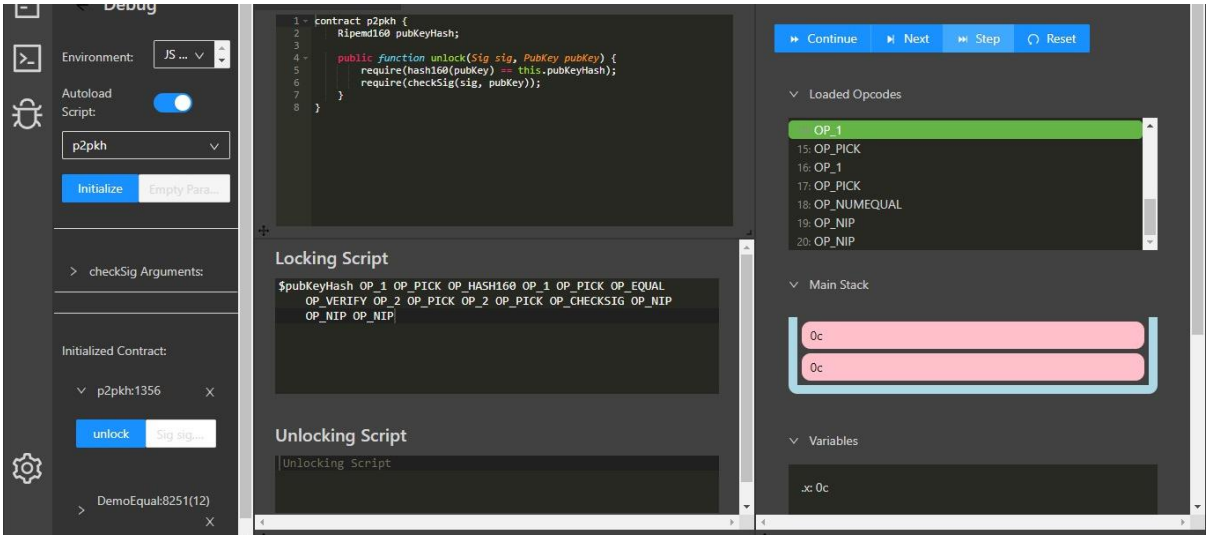
main stack dengan hasil 0c.

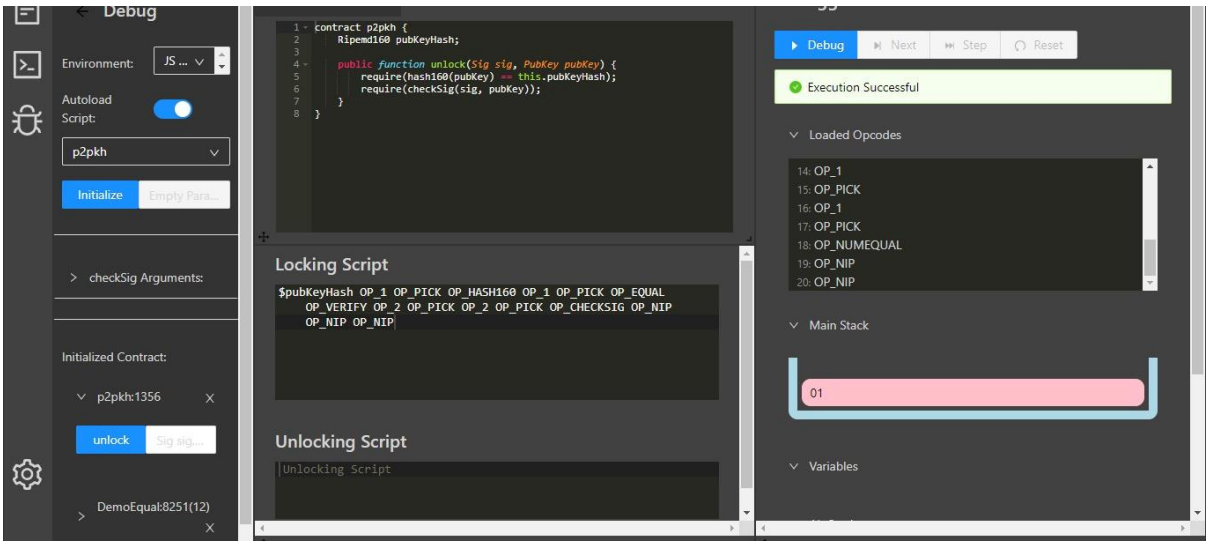


- Lalu masuk ke ripedm160 pubkeyhash dan menuju ke script OP_0, terus di periksa setiap script nya sehingga menghasil kan seperti ini :




Environment:
JS ...
Autoload Script:
p2pkh
Initialize
Empty Para...
checkSig Arguments:
Initialized Contract:
p2pkh:1356
unlock
Sig sig,...
DemoEqual:8251(12)
contract p2pkh {
Ripemd160 pubKeyHash;
public function unlock(Sig sig, PubKey pubKey) {
require(hash160(pubKey) == this.pubKeyHash);
require(checkSig(sig, pubKey));
}
}
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
Continue
Next
Step
Reset
Loaded Opcodes
00: 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,...
DemoEqual:8251(12)
contract p2pkh {
Ripemd160 pubKeyHash;
public function unlock(Sig sig, PubKey pubKey) {
require(hash160(pubKey) == this.pubKeyHash);
require(checkSig(sig, pubKey));
}
}
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
Continue
Next
Step
Reset
Loaded Opcodes
00: 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)
contract p2pkh {
Ripemd160 pubKeyHash;
public function unlock(Sig sig, PubKey pubKey) {
require(hash160(pubKey) == this.pubKeyHash);
require(checkSig(sig, pubKey));
}
}
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
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