

# EE4017 Mini Project 1

...

## Group 4

Lam Nga Wai	55235904
Tsoi Hing Chung Sunny	55216557
Mak Kai Man	54442483
Yeung Tung Yan	55213094
Yeung Yuk Ling	55220130

# Objective

This mini-project is to establish the blockchain technology to application with achieving the compulsory features and developing additional functions with Python.

---

# Compulsory Features

1. Generate a new wallet
  2. Perform Transactions
  3. Generate Coin Rewards
  4. Generate new blocks  
(proof-of-work & consensus)
  5. Peer connection & Sync the whole  
blockchain
-

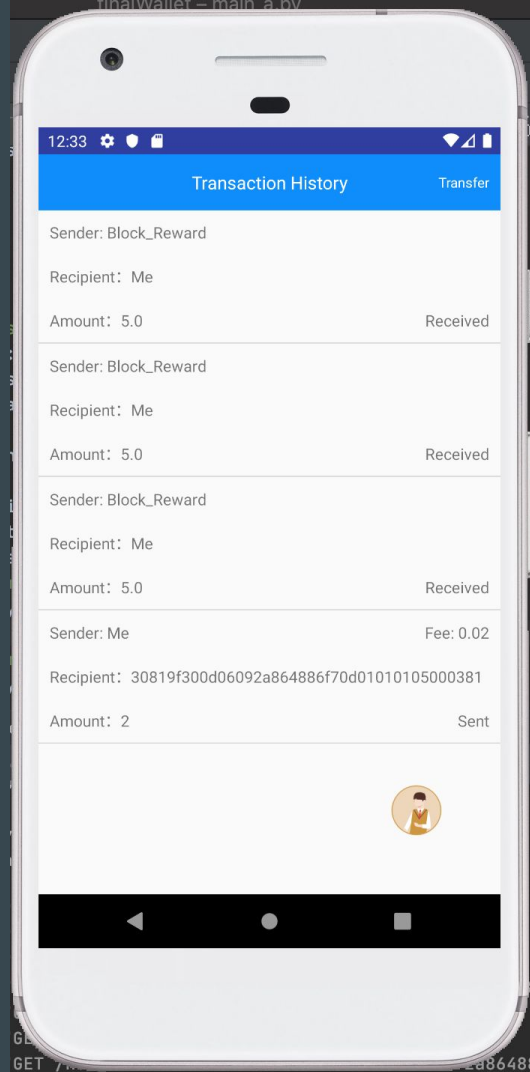
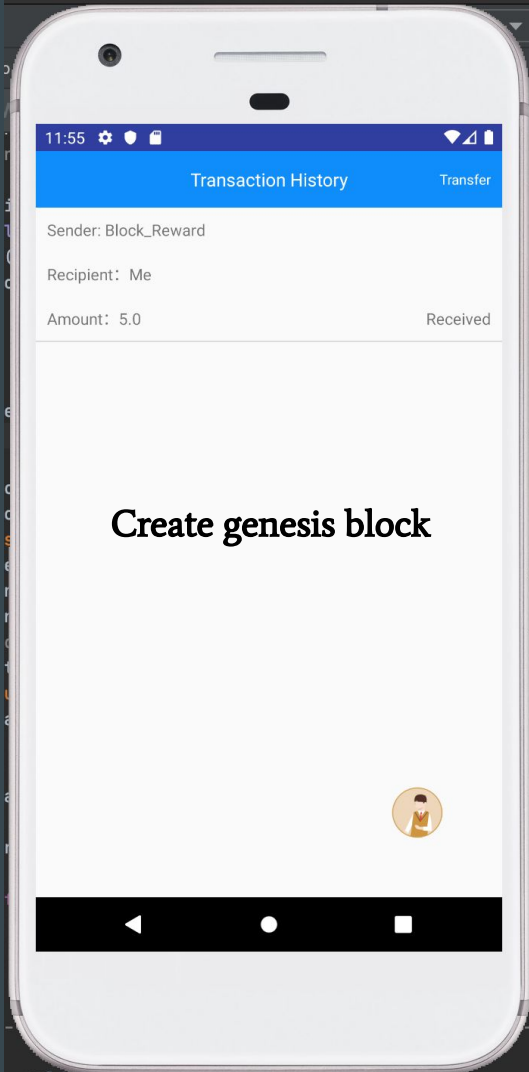
# Flow of transactions

- Generate Wallet
- Create a new blockchain and create the genesis block
- Add a signature to the transaction
- Verify the signature in the transaction
- Using mining to generate new blocks and claim the block reward.

## Genesis Block

## Signature

```
{
  "chain": "[{"index": 0, "transactions": [{"sender": "Block_Reward",
    "recipient": "30819f300d06092a864886f70d0101050003818d0030818902818100cb1b7bda6ba1fa23ed2da6caaae90af6c59df3a03ec01195c1cb5f99277abdfa27dcd7b1dc7e3e38e400d4ac261871a20530cf1ae307fd1f95550cb0a82bdfc4cc98dd6e7e299c2fa6915312318eb40e97e7fcb9977fbe79042a251a02050c9916c0e5976ebf04ae0bcb3a4669048c6f95eb3d76b1e2ecc85453ea62278eb6090203010001", "value": "5.0"}], "timestamp": "11/09/2020, 23:07:13", "previous_hash": "0", "hash": "a43645d8e56229b9359340b5995da712cdfaad164beaa868e27b816ebd787912", "nonce": 0}], [{"index": 1, "transactions": [{"sender": "Block_Reward",
    "recipient": "30819f300d06092a864886f70d0101050003818d0030818902818100cb1b7bda6ba1fa23ed2da6caaae90af6c59df3a03ec01195c1cb5f99277abdfa27dcd7b1dc7e3e38e400d4ac261871a20530cf1ae307fd1f95550cb0a82bdfc4cc98dd6e7e299c2fa6915312318eb40e97e7fcb9977fbe79042a251a02050c9916c0e5976ebf04ae0bcb3a4669048c6f95eb3d76b1e2ecc85453ea62278eb6090203010001", "value": "5.0"}], [{"sender": "30819f300d06092a864886f70d0101050003818d0030818902818100d25334b31fe792562d00f8ccb45e50eeae78f6354e174afbfdd6c90ea8517b6cde3e85277ddbcb4f088278c3651d3af35226a025134a3bdf907f0f5eaa0ebefc00514744dc532df4c46bd0428653c429fa8084dae74ca643b12f67e6db5a1e05ac973f450830b31f7da4c4b1f6c6bf3b704b0b8132e08a13a574a004edde0b7170203010001",
    "recipient": "30819f300d06092a864886f70d0101050003818d0030818902818100b017dfb47da6af4678bac642b43be89f67455267e14cdd51324270d7b194d68c47b79e8fca9077d32525393dbe1eef3bc59100f8c482ab8c7c083c71fb24cc736a2de2db2407fffd2f7ee0760648c8e43bda9f692d73e7fbd163097c8570016f773c945af9fb1dd363e355020e57aa750521d4a124d190d052d4ac392cf8c590203010001", "value": "1"}], [{"index": 2, "transactions": [{"sender": "83204e188c7acb7b2f1fd326f2a04c2c724b67a01409c457f45ddb32d941d8bd15e8c1044a444a6cb3ac8dce333b19f3f551acafdecbbbf7f2159a1478a2f7f7583bd147d347544fd4135125570c2bfb2680340fb7eb72d20acd8bcb2e1ebf1f1cc59c0bd7484d7cb8dd71e7e8e65365949a548947d3887d7483d381635cd4c69", "timestamp": "11/09/2020, 23:08:20", "previous_hash": "a43645d8e56229b9359340b5995da712cdfaad164beaa868e27b816ebd787912", "hash": "00e0e4d06b73aa96c98ab4365bba27b881c46714a35119c92e9cd055b98a5044", "nonce": 16}], "length": 2}
  ]
}
```



# Optional Features

1. Reject malformed blocks
2. Able to change difficulty when the hash power of the network change
3. Check the balance before confirming a transaction
4. Give interest to coin sholder
5. Charge transaction fee from the sender of the transaction
6. Developed a lightweight node that store block header

# Reject Malformed Blocks

- Digital Signature Validation
- Previous hash = Current hash?



# Change difficulty

- Change every 5 blocks
- Ranges from 1-6, having 3 as initial value
- Change according to the percentage of increment/decrement

```
"57c61fa7bbdbd38474b5e7482b149cd269e9f88ab461cf6e182e2982dae3c996facacbc9047985c61cd5a6aa9bd4994a6efaa249ebb357dcdb8e4cf2687d7f331205482zaf1fe3106223916d84e784cad4e7b5fedfb8ba4e688f2e374b4656a0c7b95986cc4c60a28dc3c196cd1c19013f38fbccc559408987d339fe3de115\\\"}\\\", \"timestamp\": \"'11/09/2020, 23:48:38'\", \"previous_hash\": \"'000ebf2eab388700f26bcdf378ca3b0221b539a9b1c5ce6366cf643ba46491\", \"hash\": \"'000ebf2eab388700f26bcdf378ca3b0221b539a9b1c5ce6366cf643ba46491\", \"merk1e_root\": \"'8fab6ed8c1f3024b141ec9c98a583f4951d153452fac2429475c157417244f9\", \"nonce\": 6236, \"difficulty\": 3}, {\"index\": 17, \"transactions\": [ {\"id\": \"0001f30819f30d06092a8688e67d0d10105000381d8003818902818100e0c421b4d444325f4e0a071b94f13b6a200d69b6f06518050b5dcbf737cb7d15a6eca29bf795f729eb1512aec24790b2da4f68ee81599e4b32f5e240a944caec4531d8f59224d00e531cab1d5477aed42358b142768104d5efe94a79953ff2eb032b3f7af6adeea0ca4dff07791b48aa26a3a55e5b0203010001\\\", \"value\\\": \"'1\\\", \"fee\\\": \"'0.01\\\", \"signature\\\": \"'1\\\", \"length\\\": 18} ] } ], \"length\": 18}
```

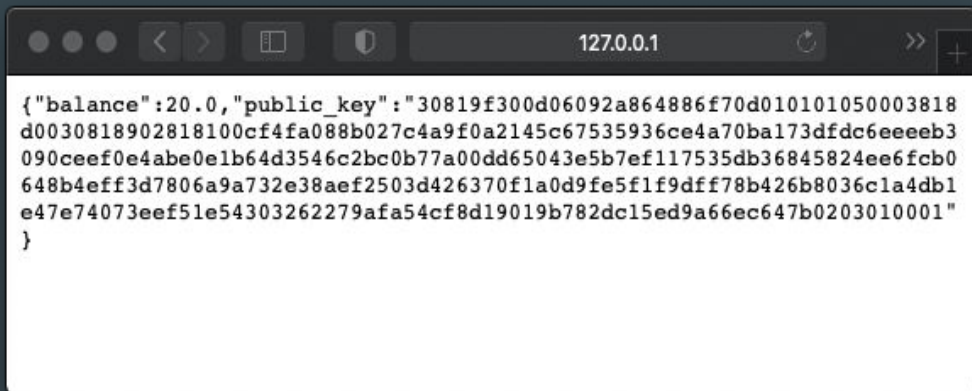
```
{"accumulated_blocks":6,"difficulty":4,"previous_time_spent":1.904389,"time_spent":2.205153,"timestamp":"Mon, 09 Nov 2020 23:48:56 GMT"}
```

# Transaction Related Features

- Reject invalid transaction
- Check balance
- Give interest
- Charge transaction fee



# Reject invalid transaction

A screenshot of a web browser window with the address bar showing '127.0.0.1'. The main content area displays a JSON object with a balance of 20.0 and a long public key.

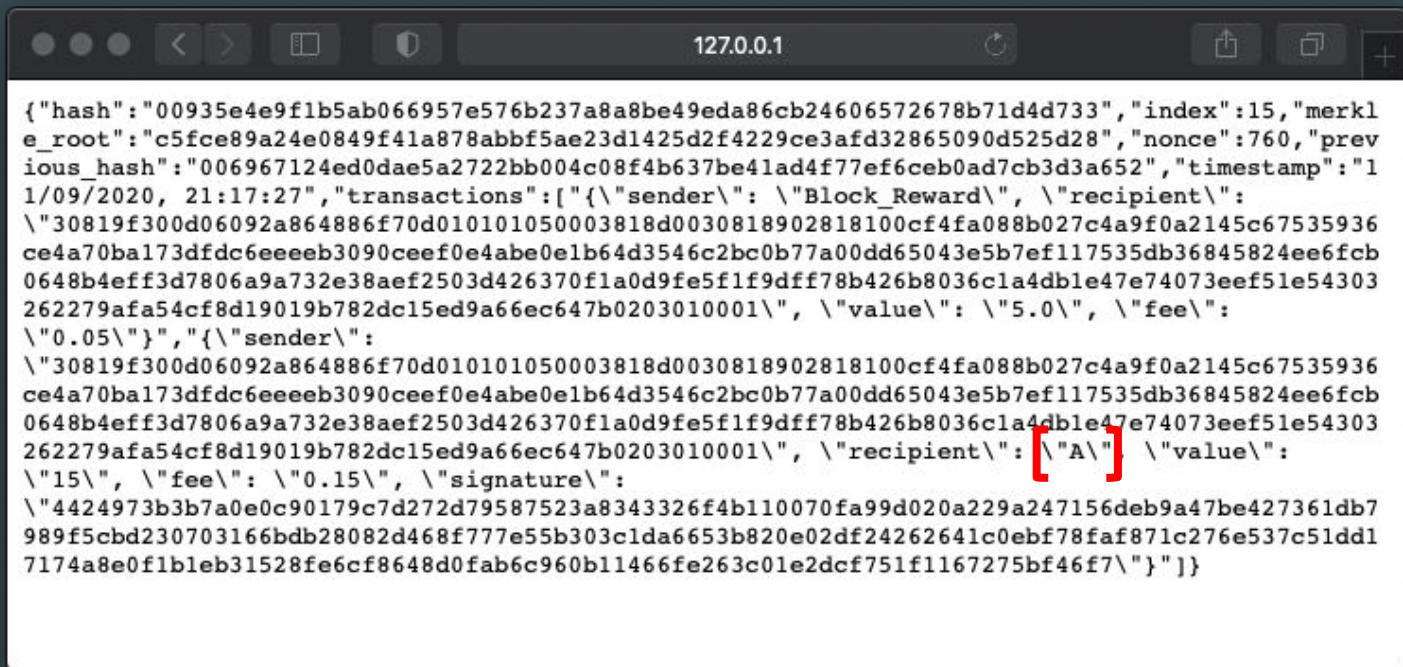
```
{ "balance": 20.0, "public_key": "30819f300d06092a864886f70d010101050003818d0030818902818100cf4fa088b027c4a9f0a2145c67535936ce4a70ba173dfdc6eeeb3090ceef0e4abe0e1b64d3546c2bc0b77a00dd65043e5b7ef117535db36845824ee6fcb0648b4eff3d7806a9a732e38aef2503d426370f1a0d9fe5f1f9dff78b426b8036c1a4db1e47e74073eef51e54303262279afa54cf8d19019b782dc15ed9a66ec647b0203010001" }
```

```
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=A&amount=15" -X POST http://127.0.0.1:5001/new_transaction
{"message": "Transaction will be added to Block "}
```

```
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=B&amount=15" -X POST http://127.0.0.1:5001/new_transaction
{"message": "Transaction will be added to Block "}
```

```
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$
```

# Reject invalid transaction



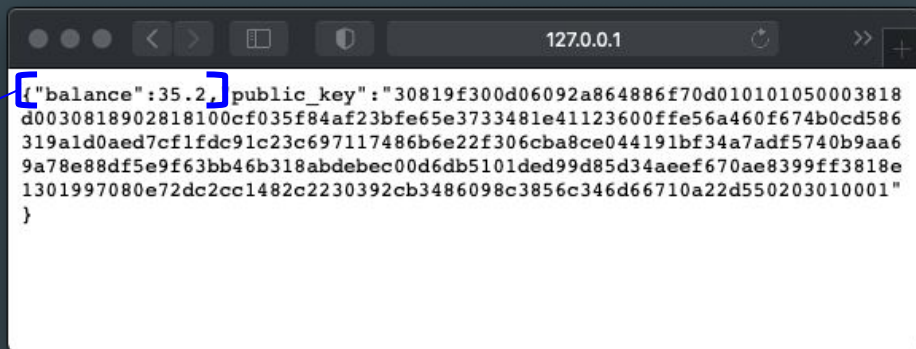
```
{
  "hash": "00935e4e9f1b5ab066957e576b237a8a8be49eda86cb24606572678b71d4d733",
  "index": 15,
  "merkle_root": "c5fce89a24e0849f41a878abbf5ae23d1425d2f4229ce3afd32865090d525d28",
  "nonce": 760,
  "previous_hash": "006967124ed0dae5a2722bb004c08f4b637be41ad4f77ef6ceb0ad7cb3d3a652",
  "timestamp": "11/09/2020, 21:17:27",
  "transactions": [
    {
      "sender": "Block_Reward",
      "recipient": "30819f300d06092a864886f70d010101050003818d0030818902818100cf4fa088b027c4a9f0a2145c67535936ce4a70ba173dfdc6eeeb3090ceef0e4abe0elb64d3546c2bc0b77a00dd65043e5b7ef117535db36845824ee6fcb0648b4eff3d7806a9a732e38aef2503d426370f1a0d9fe5f1f9dff78b426b8036cla4db1e47e74073eef51e54303262279afa54cf8d19019b782dc15ed9a66ec647b0203010001",
      "value": "5.0",
      "fee": "0.05"
    },
    {
      "sender": "30819f300d06092a864886f70d010101050003818d0030818902818100cf4fa088b027c4a9f0a2145c67535936ce4a70ba173dfdc6eeeb3090ceef0e4abe0elb64d3546c2bc0b77a00dd65043e5b7ef117535db36845824ee6fcb0648b4eff3d7806a9a732e38aef2503d426370f1a0d9fe5f1f9dff78b426b8036cla4db1e47e74073eef51e54303262279afa54cf8d19019b782dc15ed9a66ec647b0203010001",
      "recipient": "A",
      "value": "15",
      "fee": "0.15",
      "signature": "4424973b3b7a0e0c90179c7d272d79587523a8343326f4b110070fa99d020a229a247156deb9a47be427361db7989f5cbd230703166bdb28082d468f777e55b303c1da6653b820e02df24262641c0ebf78faf871c276e537c51dd17174a8e0f1b1eb31528fe6cf8648d0fab6c960b11466fe263c01e2dcf751f1167275bf46f7"
    }
  ]
}
```

```
/////////"Interest////////", ///////////"recipient////////":  
/////////"30819f300d06092a864886f70d010101050003818d0030818902818100cf035f84af23bfe65e3733481e411236  
00ffe56a460f674b0cd586319ald0aed7cf1fdc91c23c697117486b6e22f306cba8ce044191bf34a7adf5740b9aa69a78e  
88df5e9f63bb46b318abdeb00d6db5101ded99d85d34aeef670ae8399ff3818e1301997080e72dc2cc1482c2230392cb  
3486098c3856c346d66710a22d550203010001////////", ///////////"value////////": 0.5, ///////////"fee////////":
```

Add interest to the coins holder  
whenever 10 blocks were created, it is  
1% of total balance

```
/////////"fee////////": ///////////"0.05////////"}\\\\", \\\\"{/////////"sender////////":  
/////////"30819f300d06092a864886f70d010101050003818d0030818902818100cf035f84af23bfe65e3733481e411236  
00ffe56a460f674b0cd586319ald0aed7cf1fdc91c23c697117486b6e22f306cba8ce044191bf34a7adf5740b9aa69a78e  
88df5e9f63bb46b318abdeb00d6db5101ded99d85d34aeef670ae8399ff3818e1301997080e72dc2cc1482c2230392cb  
3486098c3856c346d66710a22d550203010001////////", ///////////"recipient////////": ///////////"B////////",  
/////////"value////////": ///////////"30////////", ///////////"fee////////": ///////////"0.3////////",  
/////////"signature////////":  
/////////"45a8bf4e4cf8da717a7e0900220302972c18f625d3ce77c59255270ff6f127db12293d82b271f7431736013792  
4537f2ceccde34c64f1b2ad367546008afb7a75558ffde2fc2ab34c5d9cf7b98e5bd9bf6a68cac3d71058fc16601f691c5  
f25ff1ca54d993283b8860c350c27b5ce05c206aa0387c6072eba41e0d455364ede0\\\\\\\\\\\\\\\\"}\\\\\\\\"}],
```

Charge the sender a 1% transaction  
fee for the transaction

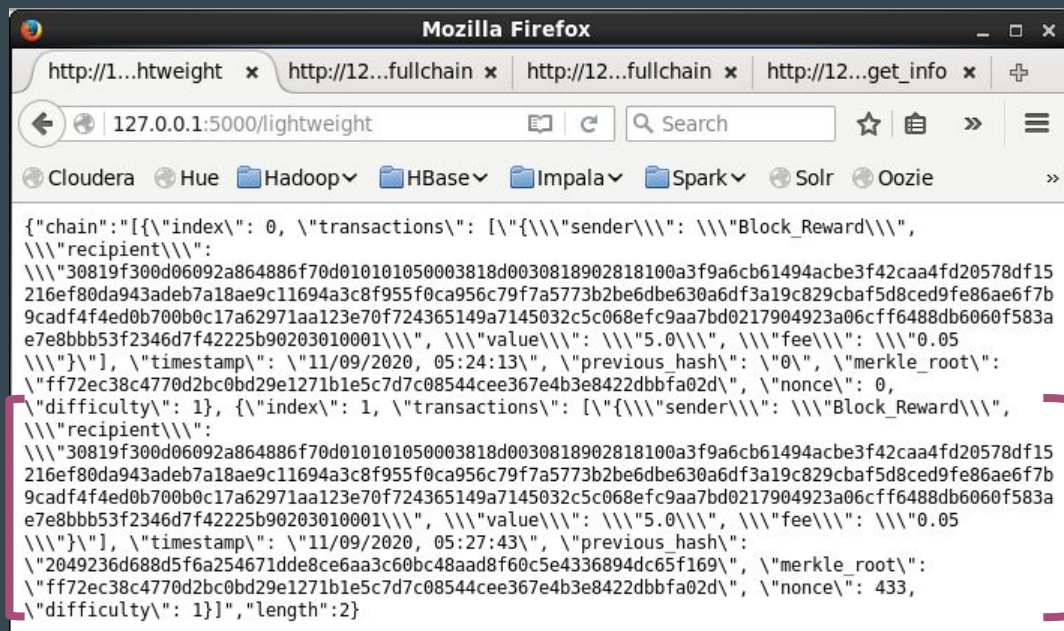


```
127.0.0.1  
{"balance":35.2,"public_key":"30819f300d06092a864886f70d010101050003818  
d0030818902818100cf035f84af23bfe65e3733481e41123600ffe56a460f674b0cd586  
319ald0aed7cf1fdc91c23c697117486b6e22f306cba8ce044191bf34a7adf5740b9aa6  
9a78e88df5e9f63bb46b318abdeb00d6db5101ded99d85d34aeef670ae8399ff3818e  
1301997080e72dc2cc1482c2230392cb3486098c3856c346d66710a22d550203010001"  
}
```

Balance after adding interest and  
charging transaction fee



# Lightweight node



```
{
  "chain": [
    {
      "index": 0,
      "transactions": [
        {
          "sender": "Block_Reward",
          "recipient": "30819f300d06092a864886f70d0101050003818d0030818902818100a3f9a6cb61494acbe3f42caa4fd20578df15216ef80da943adeb7a18ae9c11694a3c8f955f0ca956c79f7a5773b2be6dbe630a6df3a19c829cbaf5d8ced9fe86ae6f7b9cadf4f4ed0b700b0c17a62971aa123e70f724365149a7145032c5c068efc9aa7bd0217904923a06cff6488db6060f583ae7e8bbb53f2346d7f42225b90203010001",
          "value": "5.0",
          "fee": "0.05",
          "timestamp": "11/09/2020, 05:24:13",
          "previous_hash": "0",
          "merkle_root": "ff72ec38c4770d2bc0bd29e1271b1e5c7d7c08544cee367e4b3e8422dbbfa02d",
          "nonce": 0,
          "difficulty": 1
        }
      ],
      "index": 1,
      "transactions": [
        {
          "sender": "Block_Reward",
          "recipient": "30819f300d06092a864886f70d0101050003818d0030818902818100a3f9a6cb61494acbe3f42caa4fd20578df15216ef80da943adeb7a18ae9c11694a3c8f955f0ca956c79f7a5773b2be6dbe630a6df3a19c829cbaf5d8ced9fe86ae6f7b9cadf4f4ed0b700b0c17a62971aa123e70f724365149a7145032c5c068efc9aa7bd0217904923a06cff6488db6060f583ae7e8bbb53f2346d7f42225b90203010001",
          "value": "5.0",
          "fee": "0.05",
          "timestamp": "11/09/2020, 05:27:43",
          "previous_hash": "2049236d688d5f6a254671dde8ce6aa3c60bc48aad8f60c5e4336894dc65f169",
          "merkle_root": "ff72ec38c4770d2bc0bd29e1271b1e5c7d7c08544cee367e4b3e8422dbbfa02d",
          "nonce": 433,
          "difficulty": 1
        }
      ],
      "length": 2
    }
  ]
}
```

It downloads the block headers only to validate the authenticity of the transactions

A method called Simplified payment verification (SPV) is used to verify transactions

# Merkle Tree validation

```
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=a&amount=1" -X POST http://127.0.0.1:5001/new_transaction {"message":"Transaction will be added to Block "}
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=b&amount=1" -X POST http://127.0.0.1:5001/new_transaction {"message":"Transaction will be added to Block "}
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=c&amount=1" -X POST http://127.0.0.1:5001/new_transaction {"message":"Transaction will be added to Block "}
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "recipient_address=d&amount=1" -X POST http://127.0.0.1:5001/new_transaction
```

```
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$ curl -d "sender=30819f300d06092a864886f70d010101050003818d0030818902818100d3cd7f336445e95c5345a064edf63e219fd5e7b9f4e4e5375ffad321c0294ec9e6ea49b713b6bca6392ca179590e081e3f76e364c919f201fd4b0a1ff0912cc314eb7a257daf85b49d7797dff8a1972cf108ae782b8db76f4dfd236e92fe85d1b02abb5c20977c4f90550606264b3b20fcdb4e1f6fac5025d881786ecfcb70203010001&recipient=d&svalue=1" -X POST http://127.0.0.1:5001/merkle_path [{"0","7ded0f22a61d0bcd3df77f15fd19f070ea278438a99629c9d0d63b3eb10cdaf4"}, {"0","5f358d975cdc298bf7c548498fdffdd6f6c03ff83cc08ce99ea744866b13f5ab"}, {"1","5ac870d56d3ec3f486f6063736d2fc33f12ac4998954ed9fcbdb3a64b4a3330b"}]
(venv) (base) KaydenMakde-MacBook-Pro:EE4015Miniproject kaydenmak$
```

# Job Division

## -Lam Nga Wai -

- Generate a new wallet(20%)
- Perform Transactions(20%)
- Generate Coins Reward(20%)
- Generate New Blocks(20%)
- Broadcast new blocks to the rests of connected peers(20%)
- Connect peers(20%)
- Sync the whole blockchain (50%)
- Update and check balance(50%)
- Change difficulty as the hash power of the network change

## - Tsoi Hing Chung Sunny -

- Generate a new wallet(20%)
- Perform Transactions(20%)
- Generate Coins Reward(20%)
- Generate New Blocks(20%)
- Broadcast new blocks to the rests of connected peers
- Connect peers(20%)
- Merkle tree hashing (50%)
- Lightweight node development

## - Mak Kai Man -

- Generate a new wallet(20%)
- Perform Transactions(20%)
- Generate Coins Reward(20%)
- Generate New Blocks(20%)
- Broadcast new blocks to the rests of connected peers(20%)
- Connect peers(20%)
- Sync the whole blockchain(50%)
- Reject invalid transaction
- Update and check balance(50%)
- Give interests to coins header
- Merkle tree hashing(50%)



# Job Division

## - Yeung Tung Yan -

- Generate a new wallet(20%)
- Perform Transactions(20%)
- Generate Coins Reward(20%)
- Generate New Blocks(20%)
- Broadcast new blocks to the rests of connected peers(20%)
- Connect peers(20%)
- Replace curl commands with http
- Develop node for app
- Develop an Android app on Android Studio

## - Yeung Yuk Ling -

- Generate a new wallet(20%)
- Perform Transactions(20%)
- Generate Coins Reward(20%)
- Generate New Blocks(20%)
- Broadcast new blocks to the rests of connected peers(20%)
- Connect peers(20%)
- Charge transaction fee from the sender of the transaction

Q&A