Solving Privacy and Security issues in Electronic Health Record (EHR) using Blockchain

Abstract:
The advantages of electronic health records in the clinical setting are numerous and important. In the 2012 edition of the Physician Sentiment IndexTM More than two-thirds said an EHR can actually improve patient care. Poor EHR system design and improper use can cause EHR-related errors that jeopardize the integrity of the information in the EHR, leading to errors that endanger patient safety or decrease the quality of care and EHR systems faces problems regarding data security, privacy issues and information asymmetry. We have leveraged blockchain technology to transform the EHR systems and could be a solution for the above issues.

Problems in existing EHR system:

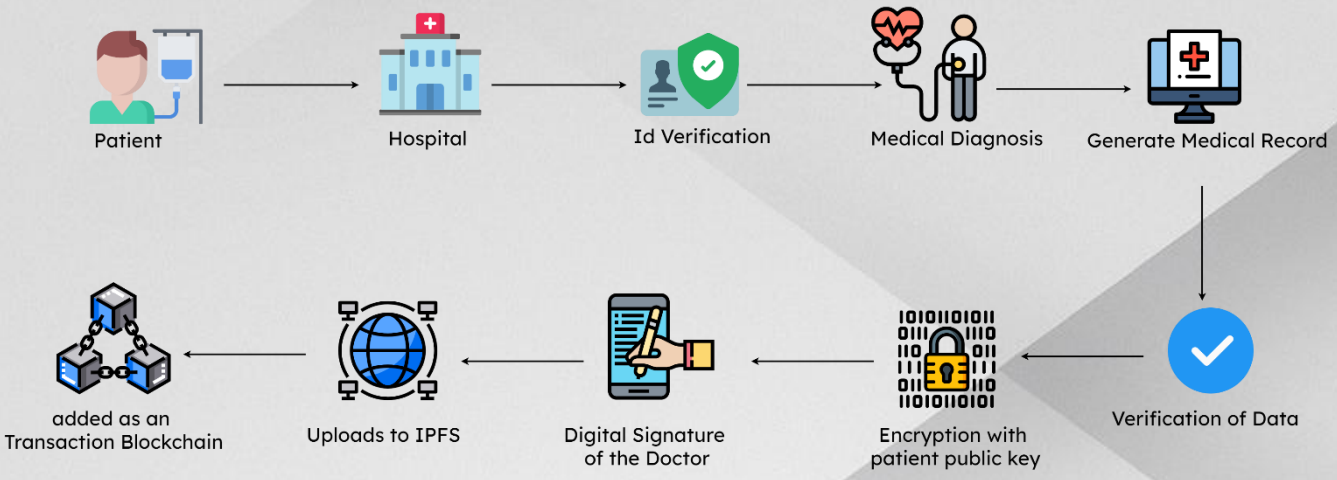
- ***Interoperability:*** It is the way for different information systems to exchange information between them.
- ***Information Asymmetry:*** which refers to one party having better access to information than the other party.
- ***Data Breaches:*** Data breaches in healthcare sector also calls for the need of a better platform.

Solution:

- We present a technique where we've leveraged the blockchain technology to transform the EHR systems and could be a solution for the above issues.
- The aim of our solution is firstly to implement blockchain technology for EHR and to give back the control of the Medical data to the patients. Moreover, we've also presented a solution for the scalability problem faced by the blockchain using ***off-chain decentralized storage*** for storing the EHR data.
- Another main issue in the traditional framework is, our EHR data is ***accessed and shared*** with unauthorized Personnel.
- Hence, we have designed a framework for sharing of EHR which is ***solely controlled by the patient*** to whom the EHR data belongs to and in order to keep the track of old EHR's we are going to implement git like, version control system on top of the IPFS.
- Data in our system can only be accessed by the patient's private key, even if someone obtains data from the decentralized storage, data will be unreadable and patients have full control over accessing their healthcare data, patients will control who sees their data and what they see. Hence, there's a reduced risk of errors, and better patient care. We believe, that the above solution will definitely improve our current Healthcare industry
- We have ensured decentralization in every flow of the system. Hence, there is ***no single point of failure***.

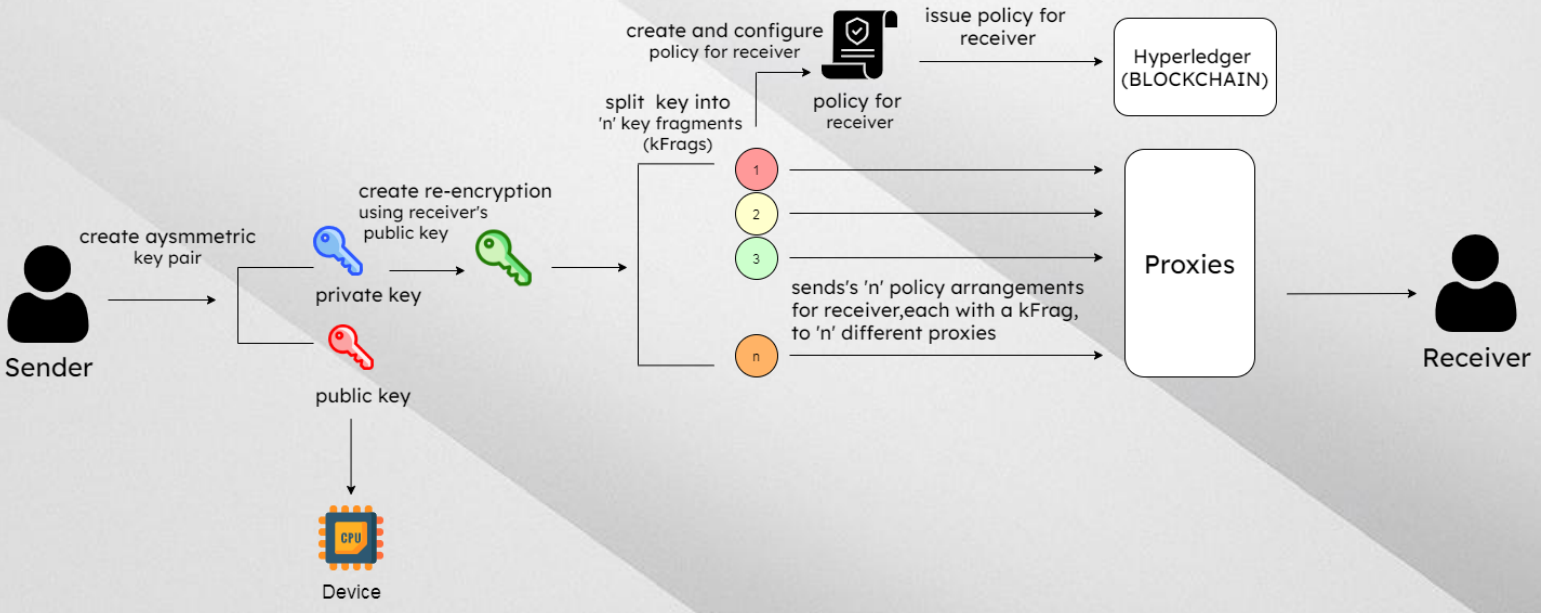
Detailed workflow:
https://prezi.com/q9x25xhgmsrv/ehr-implementation-using-blockchain/

Overall System workflow



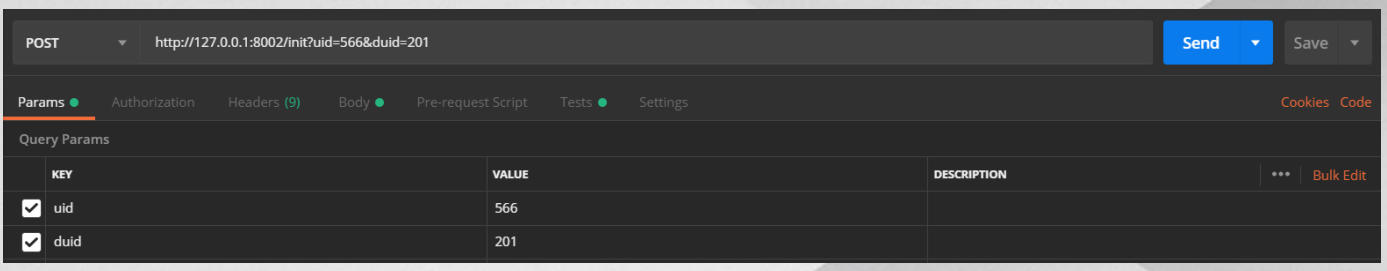
How data gets stored in our system?

How our data sharing mechanism works?

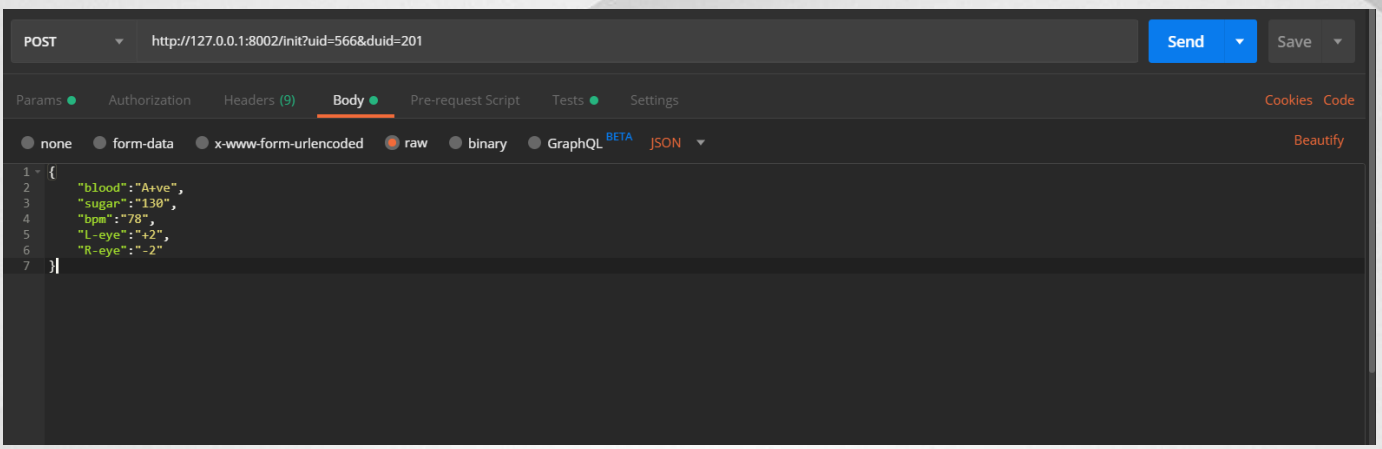


Documentation and Screenshots:

BACKEND:



Generating a new key pair for patient and doctor

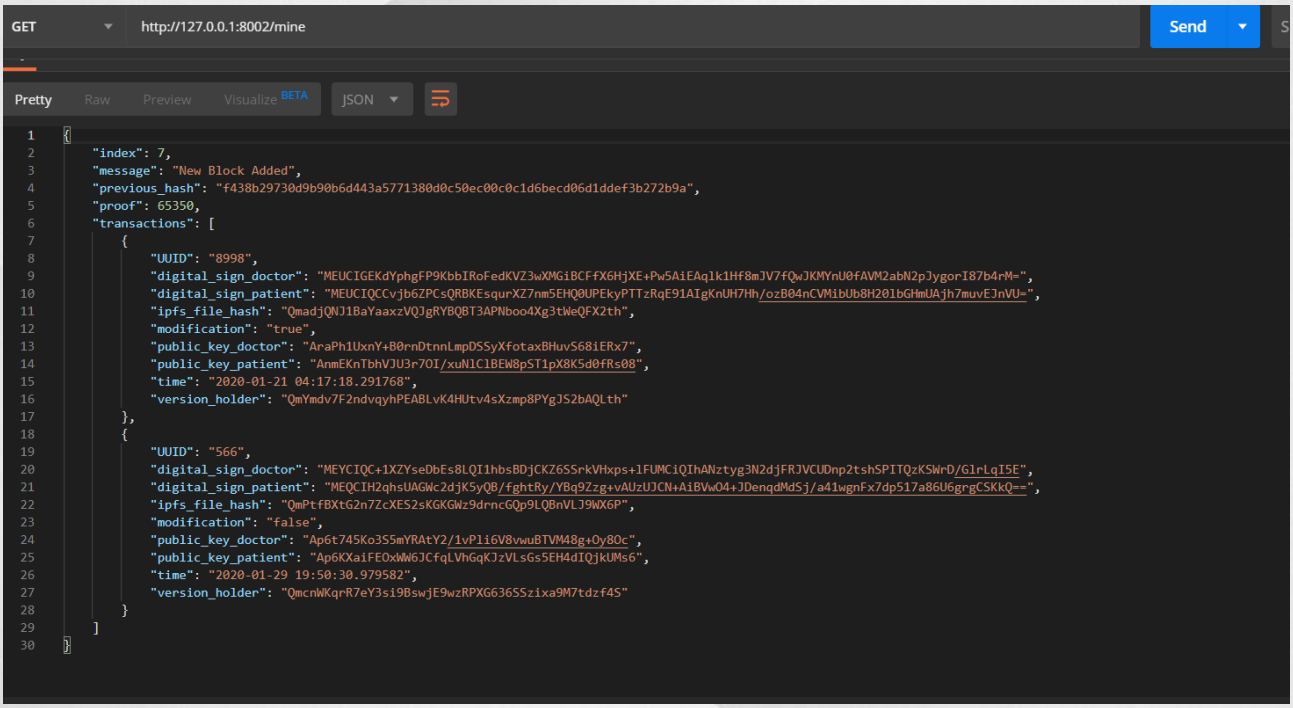


Sample EHR data

Version holder of a patient

```
{
  "8998": "QmadjQNJ1BaYaaxzVQJgRYBQBT3APNboo4Xg3tWeQFX2th",
  "999": "QmRoZNhCvG85rz8jGryvyRaGVEKDZ59LEKU9Ji7hmeenD9",
  "500": "QmejTr9MaFyZdHq3SzqYghTUPPE23QUDyL4YboEGCkcuSJ",
  "100": "QmNxpJLhPQeAKuDEarV8f3aSpMnaAviT8uo7w6F9BYNHLq",
  "997": "QmcUwg66VzR3ufiAkGM5kpR773tAvW6YobvFKfWNxhhi22",
  "222": "QmRcBLZSbeUCXfuaXAMFWeCSokJ64SDmn3SHsD997NmwRS",
  "10000": "QmdG8W9eCPB76kcsQdBYJwF33EgHRUArpAH25ZioZ4SREM",
  "400": "QmSJkuTN2qevDu6dc7yr3vt8pWk3oF8UC4LKk8np5mKpDe",
  "1001": "QmQfWRqzNCxxJKm6UstzcU4FEy9QC4JE6rLuhuhQ3Z4Beh",
  "123": "QmQp5VsKdzWPrFgBRFWFVsy1L9hxVE47PoZBA3XzyQJcCb",
  "566": "QmTXu5NMZUkq4ZqJRnfBygLVQA9j7U6UPvQA9sDJ3pR14Q"
}
```


EHR hash link of few patient (id:hash_link)




```
{
    "index": 7,
    "message": "New Block Added",
    "previous_hash": "f438b29730d9b90b6d443a5771380d0c50ec00c0c1d6becd06d1ddef3b272b9a",
    "proof": 65350,
    "transactions": [
        {
            "UUID": "8998",
            "digital_sign_doctor": "MEUCIGEKdYphgFP9KbbIRoFedKVZ3wXMGiBCFfX6HjXE+Pw5AiEAqlk1Hf8mJV7fQwJKMYnU0fAVM2abN2pJygorI87b4rM=",
            "digital_sign_patient": "MEUCIQCCvjb6ZPCsQRBKEsqurXZ7nm5EHQ0UPEkyPTTzRqE91AIgKnUH7Hh/ozB04nCVMibUb8H20lbGHmUAjh7muvEJnVU=",
            "ipfs_file_hash": "QmadjQNJ1BaYaaxzVQJgRYBQBT3APNboo4Xg3tWeQFX2th",
            "modification": "true",
            "public_key_doctor": "AraPh1UxnY+B0rnDtnnLmpDSSyXfotaxBHuvS68iERx7",
            "public_key_patient": "AnmEKnTbhVJU3r7OI/xuNlClBEW8pST1pX8K5d0fRs08",
            "time": "2020-01-21 04:17:18.291768",
            "version_holder": "QmYmdv7F2ndvqyhPEABLvK4HUtv4sXzmp8PYgJS2bAQLth"
        },
        {
            "UUID": "566",
            "digital_sign_doctor": "MEYCIQC+1XZYseDbEs8LQI1hbsBDjCKZ6SSrkVHxps+1FUMCiQIhANztyg3N2djFRJVCUDnp2tshSPITQzKSWrD/GlrLqI5E",
            "digital_sign_patient": "MEQCIH2qhsUAGWc2djK5yQB/fghtRy/YBq9Zzg+vAUzUJCN+AiBVwO4+JDenqdMdSj/a41wgnFx7dp517a86U6grgCSKkQ==",
            "ipfs_file_hash": "QmPtfBXtG2n7ZcXES2sKGKGWz9drncGQp9LQBnVLJ9WX6P",
            "modification": "false",
            "public_key_doctor": "Ap6t745Ko3S5mYRAtY2/1vPli6V8vwuBTVM48g+Oy8Oc",
            "public_key_patient": "Ap6KXaiFEOxWW6JCfqlVhGqKJzVLsGs5EH4dIQjkUMs6",
            "time": "2020-01-29 19:50:30.979582",
            "version_holder": "QmcnWKqrR7eY3si9BswjE9wzRPXG636SSzixa9M7tdzf4S"
        }
    ]
}
```

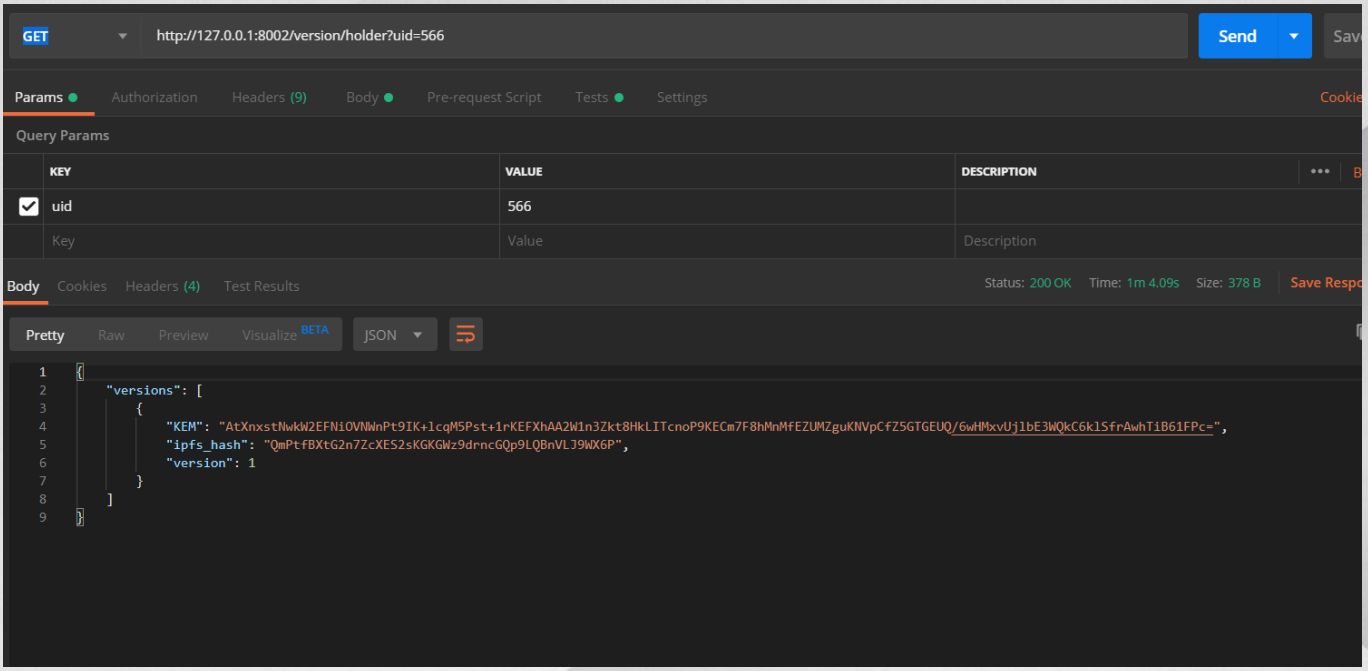

Mining

```
  File "C:\Users\Nandu\Anaconda3\lib\sit

(base) C:\Users\Nandu\Desktop\projects\m
Enter port no : 800
 * Serving Flask app "main_blockchain" (

(base) C:\Users\Nandu\Desktop\projects\m
Enter port no : 8002
 * Serving Flask app "main_blockchain" (
 * Environment: production
   WARNING: This is a development server
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://127.0.0.1:8002/ (Pr
checking
Generating key pair
checking
200_doc key pair exists and is readable
127.0.0.1 - - [29/Jan/2020 19:44:56] "GE
New Transaction initiated....
Encryption in progress
uploading.... to ipfs
hash of the file : QmQp5VsKdzWPrFgBRFWFV
hash_indices.json exists and is readable
updating.... hash indices
ipns hash=
[2020-01-29 19:45:20,595] ERROR in app:
Traceback (most recent call last):
```

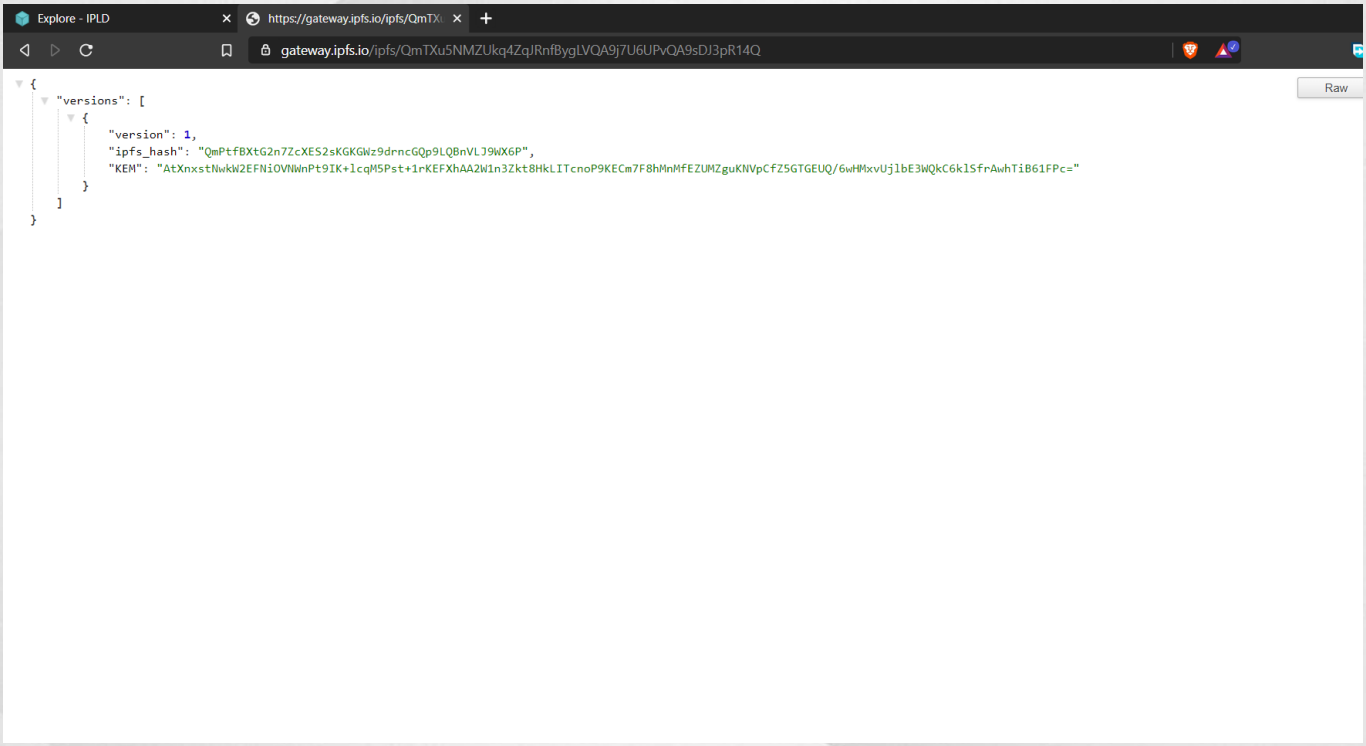
Background logs-1

```
Generating key pair
127.0.0.1 - - [29/Jan/2020 19:48:29] "PO
New Transaction initiated....
Encryption in progress
uploading.... to ipfs
hash of the file : QmPtfBXtG2n7ZcXES2sKG
hash_indices.json exists and is readable
updating.... hash indices
ipns_hash_indices.json exists and is rea
updating.... ipns hash indices
ipns hash=
566_version_holder.json exists and is re
uploading.... to ipfs
hash of the file : QmTXu5NMZUkq4ZqJRnfBy
hash_indices.json exists and is readable
updating.... hash indices
The static ipns hash :
ipns key(version holder) and newly uploa
Signing the File
Signing the File
UmbralPublicKey:029eadef8e4aa37
UmbralPublicKey:029e8a5da88510e
127.0.0.1 - - [29/Jan/2020 19:50:30] "POST /transactions/new HTTP/1.1" 201 -
127.0.0.1 - - [29/Jan/2020 19:55:18] "POST /mine HTTP/1.1" 405 -
127.0.0.1 - - [29/Jan/2020 19:55:21] "GET /mine HTTP/1.1" 200 -
checking version holder data
127.0.0.1 - - [29/Jan/2020 19:57:07] "GET /version/holder?uid=566 HTTP/1.1" 200 -
```

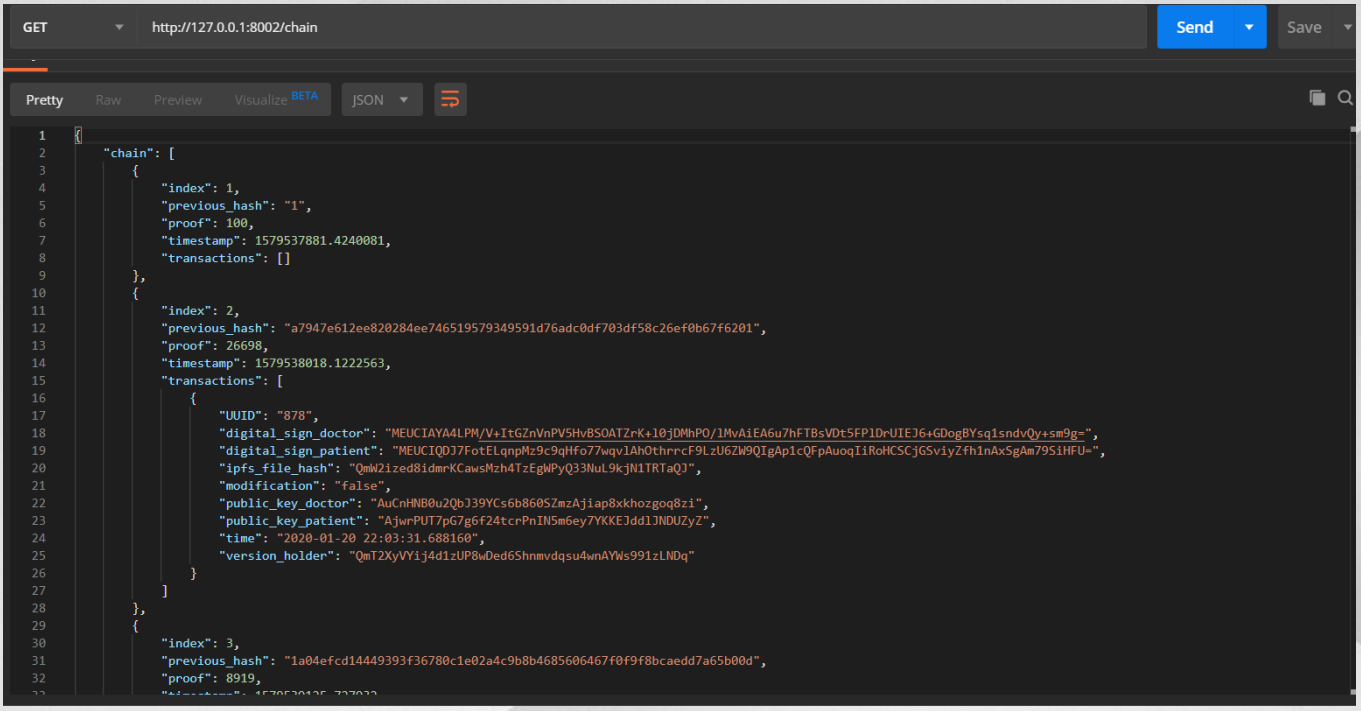
Background logs-2



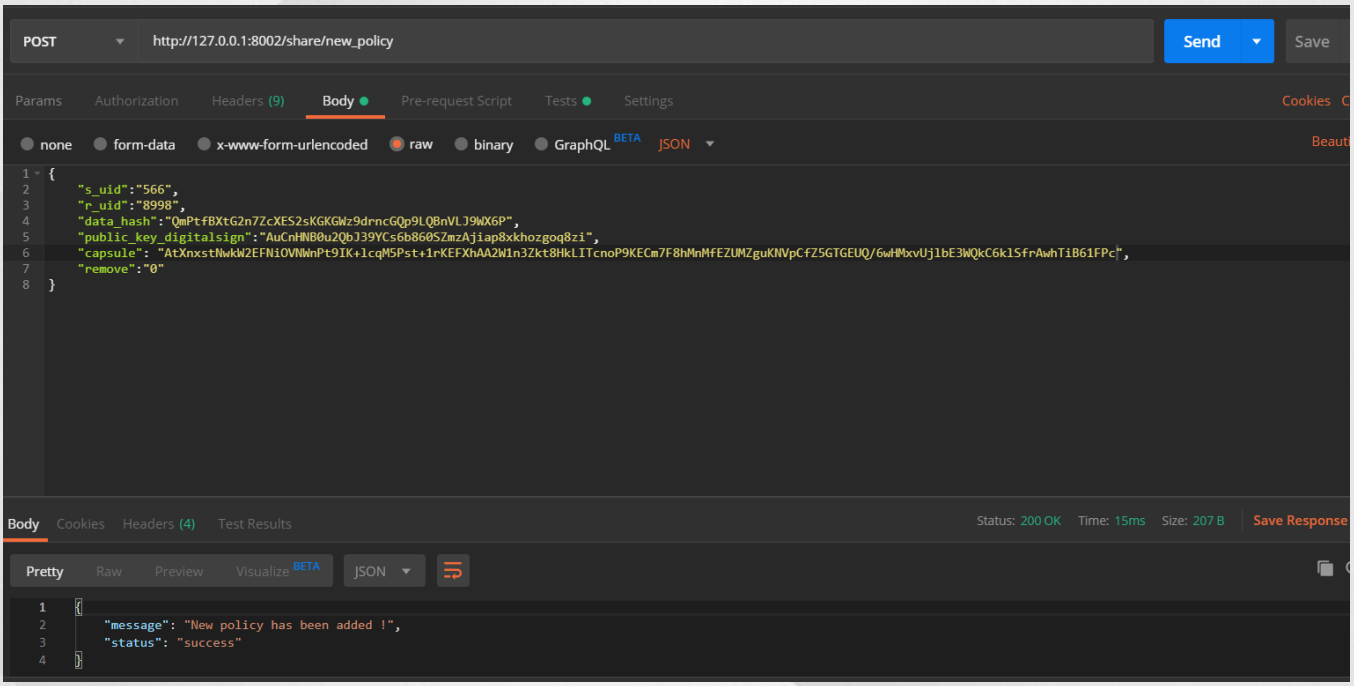
Requesting the version holder of a patient



Viewing our data from the real IPFS endpoint



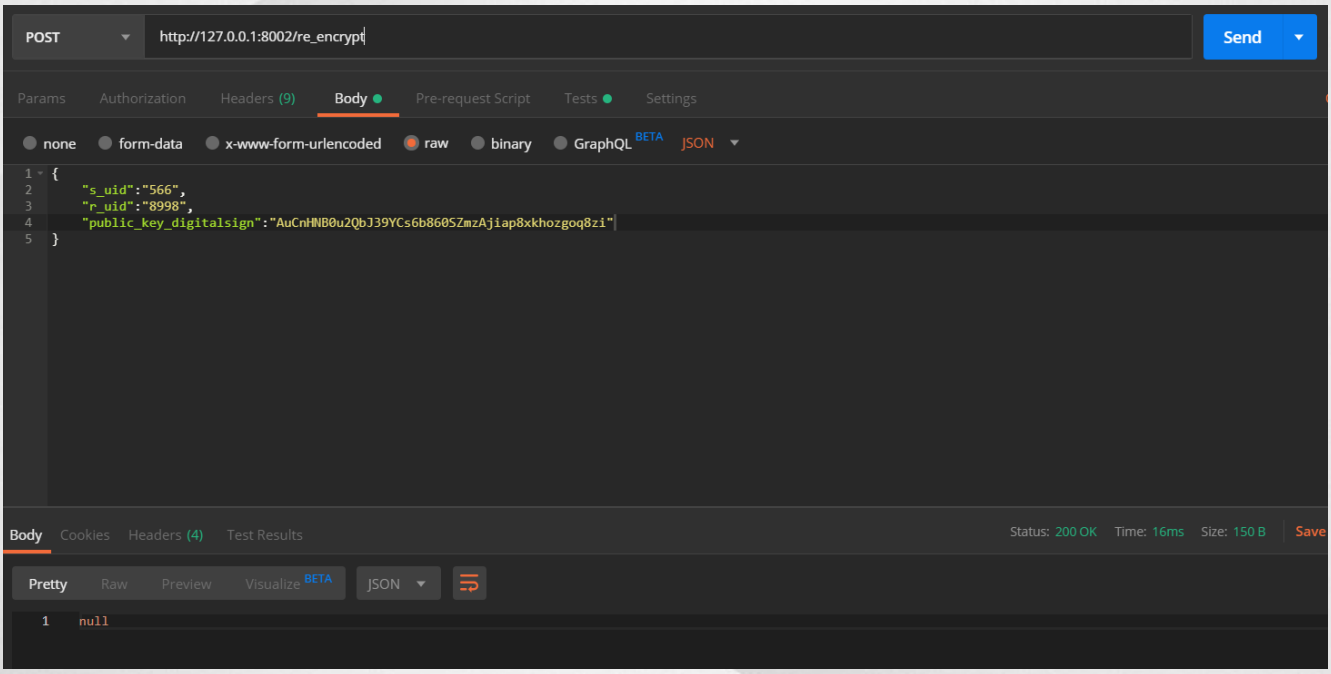
Blockchain data of a single node



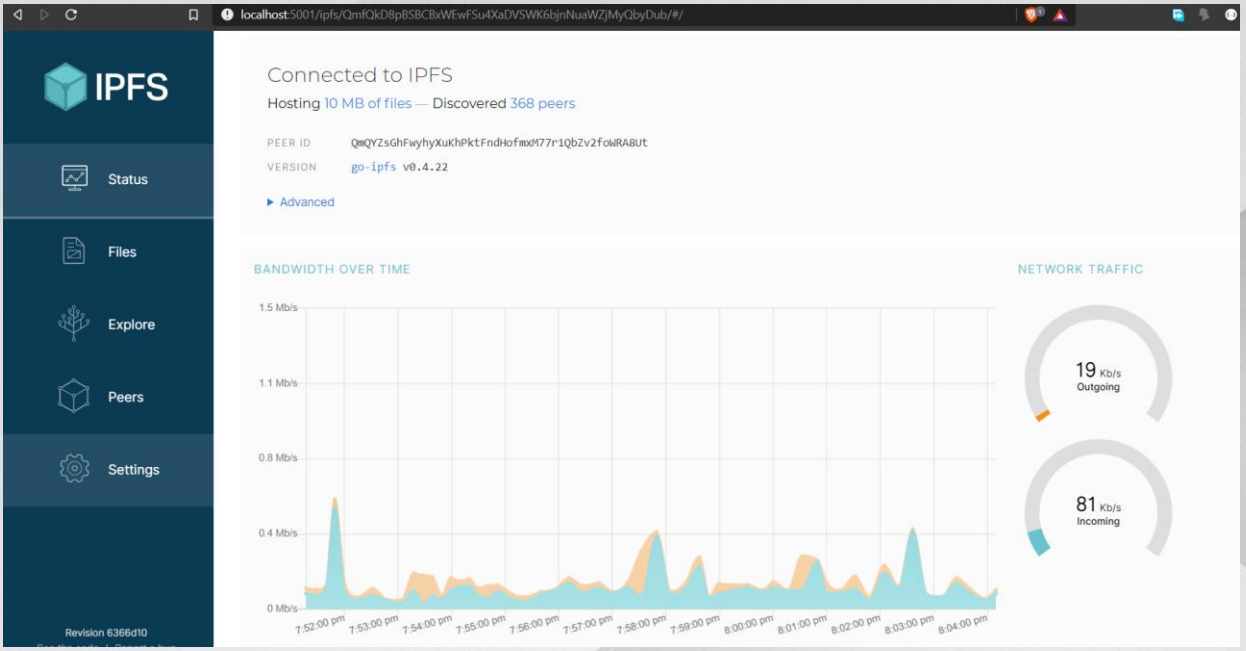
Creating a new policy for data sharing

```
hash_indices.json exists and is readable
updating.... hash indices
The static ipns hash :
ipns key(version holder) and newly uploa
Signing the File
Signing the File
UmbralPublicKey:029eadef8e4aa37
UmbralPublicKey:029e8a5da88510e
127.0.0.1 - - [29/Jan/2020 19:50:30] "POST /transactions/new HTTP/1.1" 201 -
127.0.0.1 - - [29/Jan/2020 19:55:18] "POST /mine HTTP/1.1" 405 -
127.0.0.1 - - [29/Jan/2020 19:55:21] "GET /mine HTTP/1.1" 200 -
checking version holder data
127.0.0.1 - - [29/Jan/2020 19:57:07] "GET /version/holder?uid=566 HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 19:58:40] "GET /chain HTTP/1.1" 200 -
data_sharing_policies.json exists and is readable
Modifying ploicies
127.0.0.1 - - [29/Jan/2020 20:01:45] "POST /share/new_policy HTTP/1.1" 200 -
in share
Policy not found !
```

Background logs-3



Requesting for data re-encryption



Connection details of a single Hospital (node)

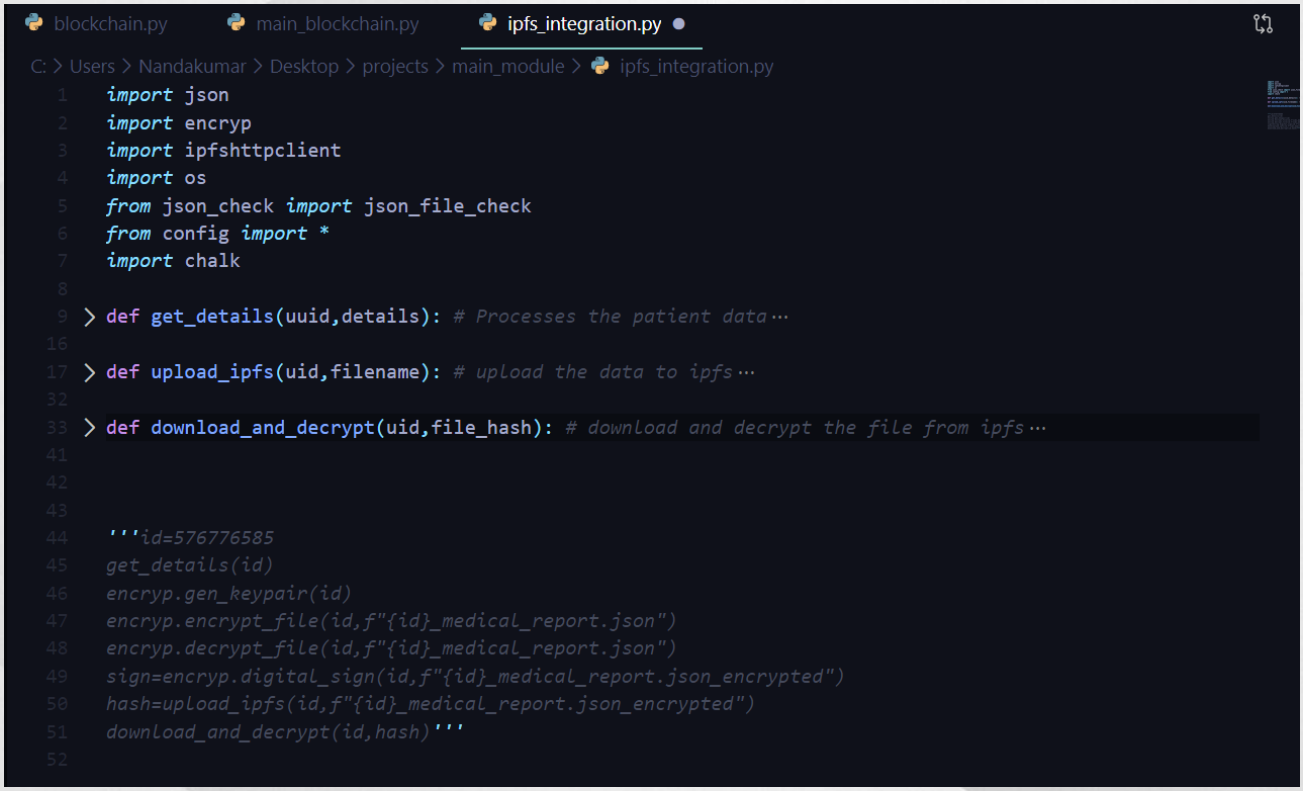
Sample Code screenshots (this is not full code):

Blockchain (code)-1

Blockchain (code)-2

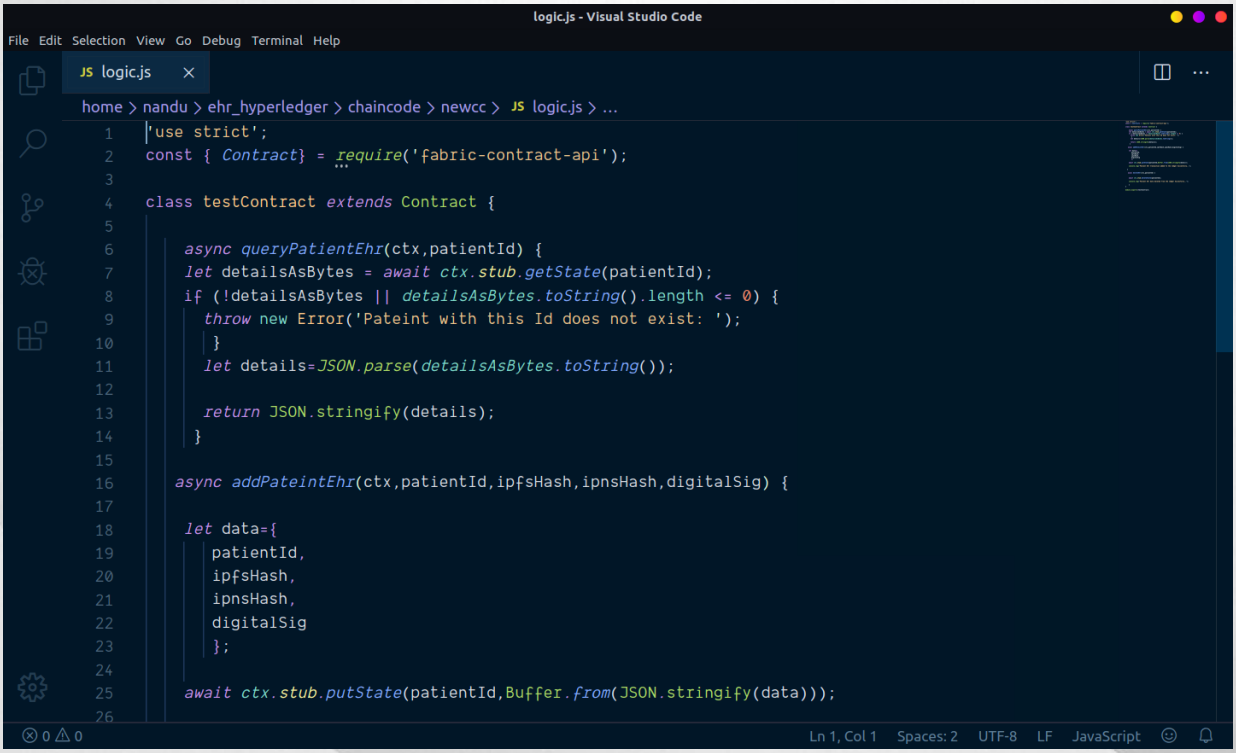
Code for interacting with the blockchain-1

Code for interacting with the blockchain-2

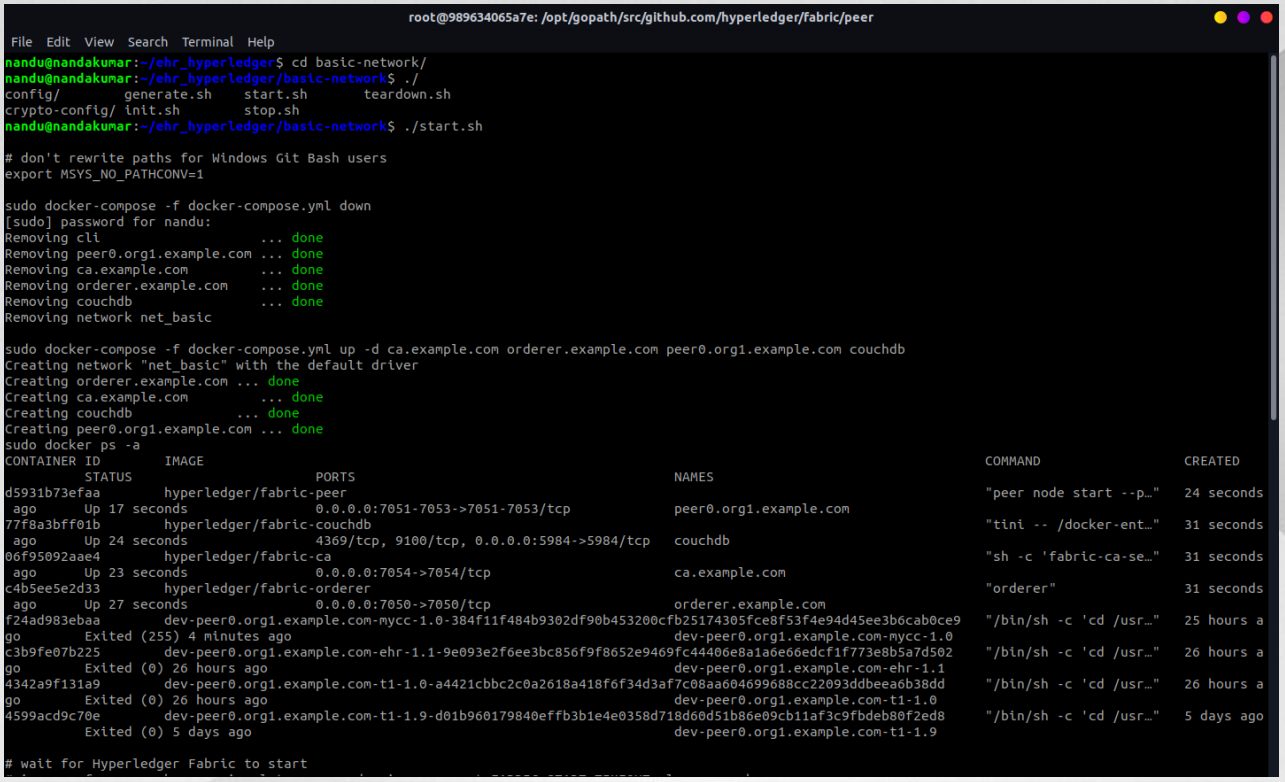


Code for interaction with the IPFS

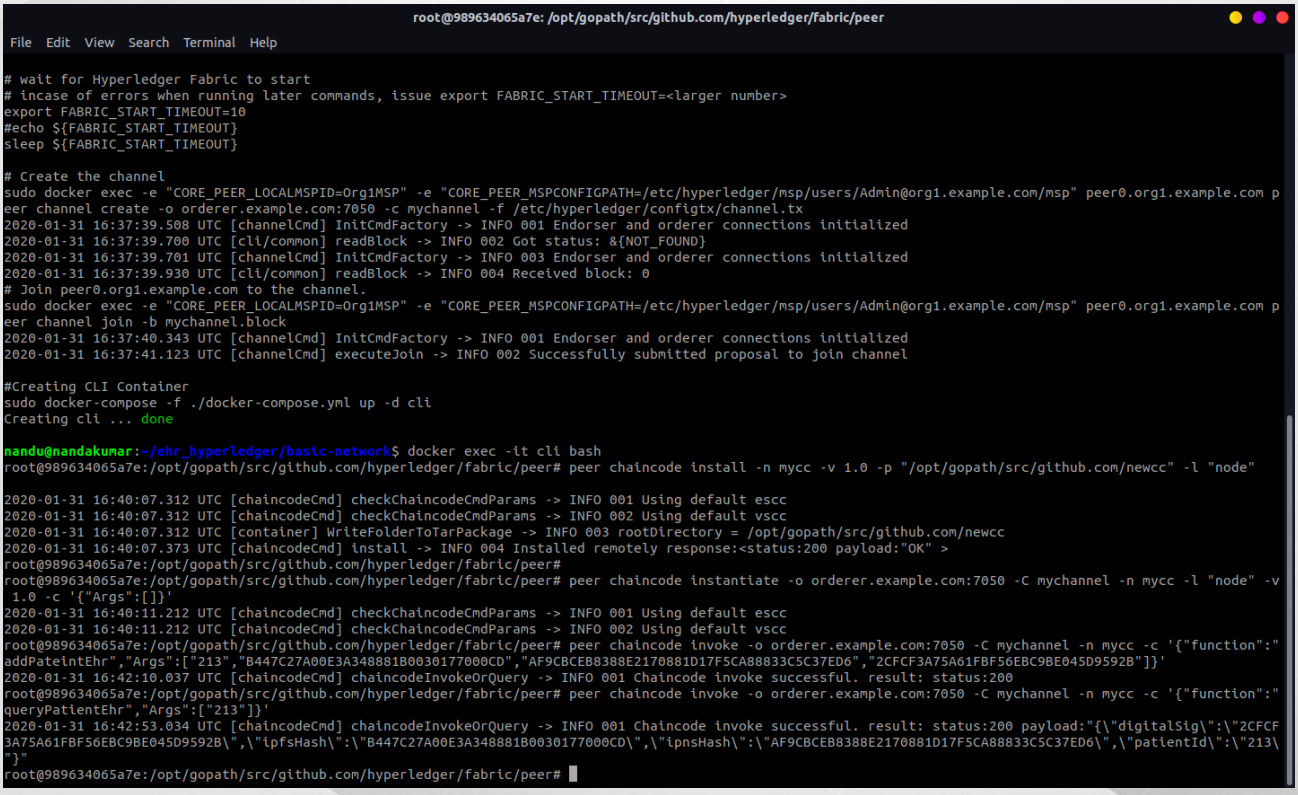
Code for Handling the logics behind versioning of HER



Sample Hyperledger Fabric EHR Chaincode

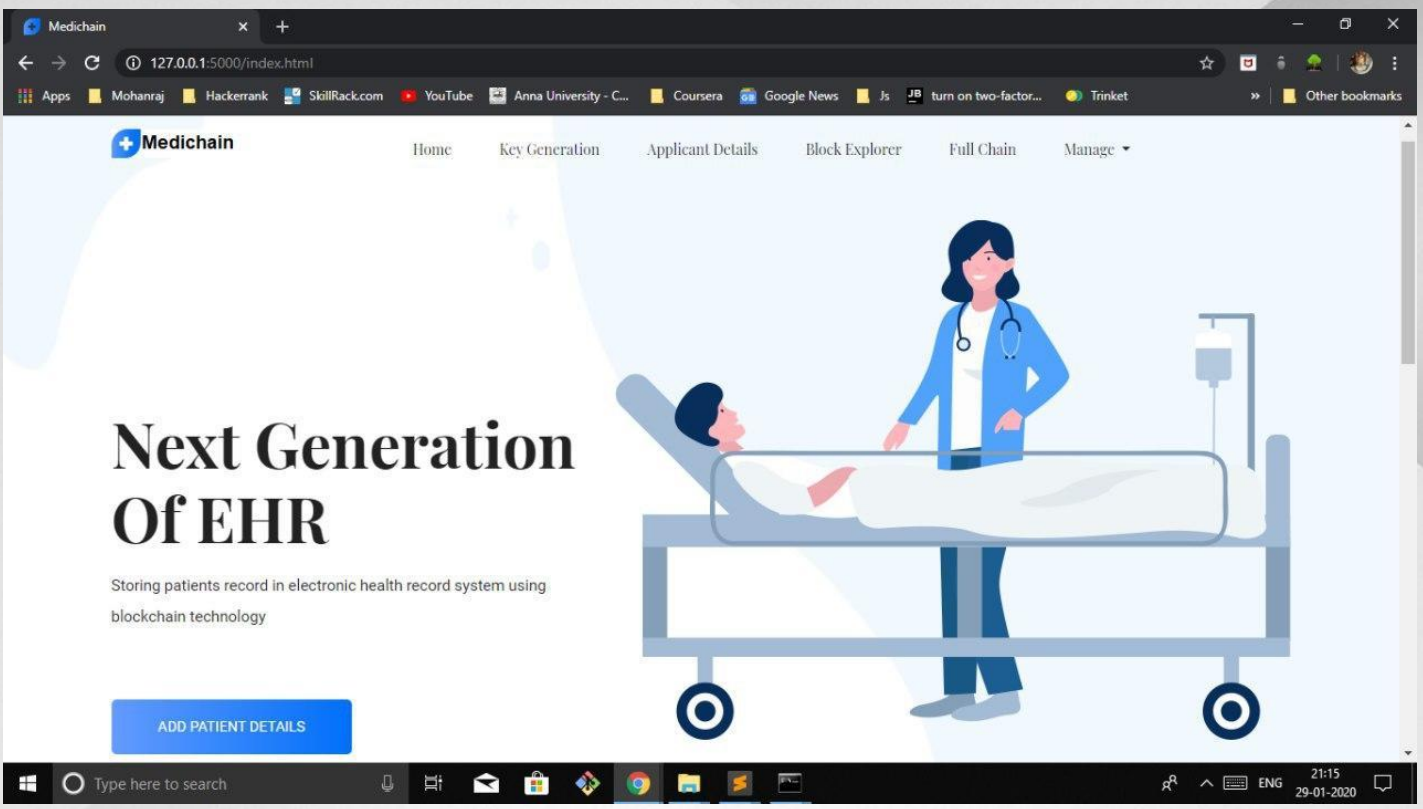


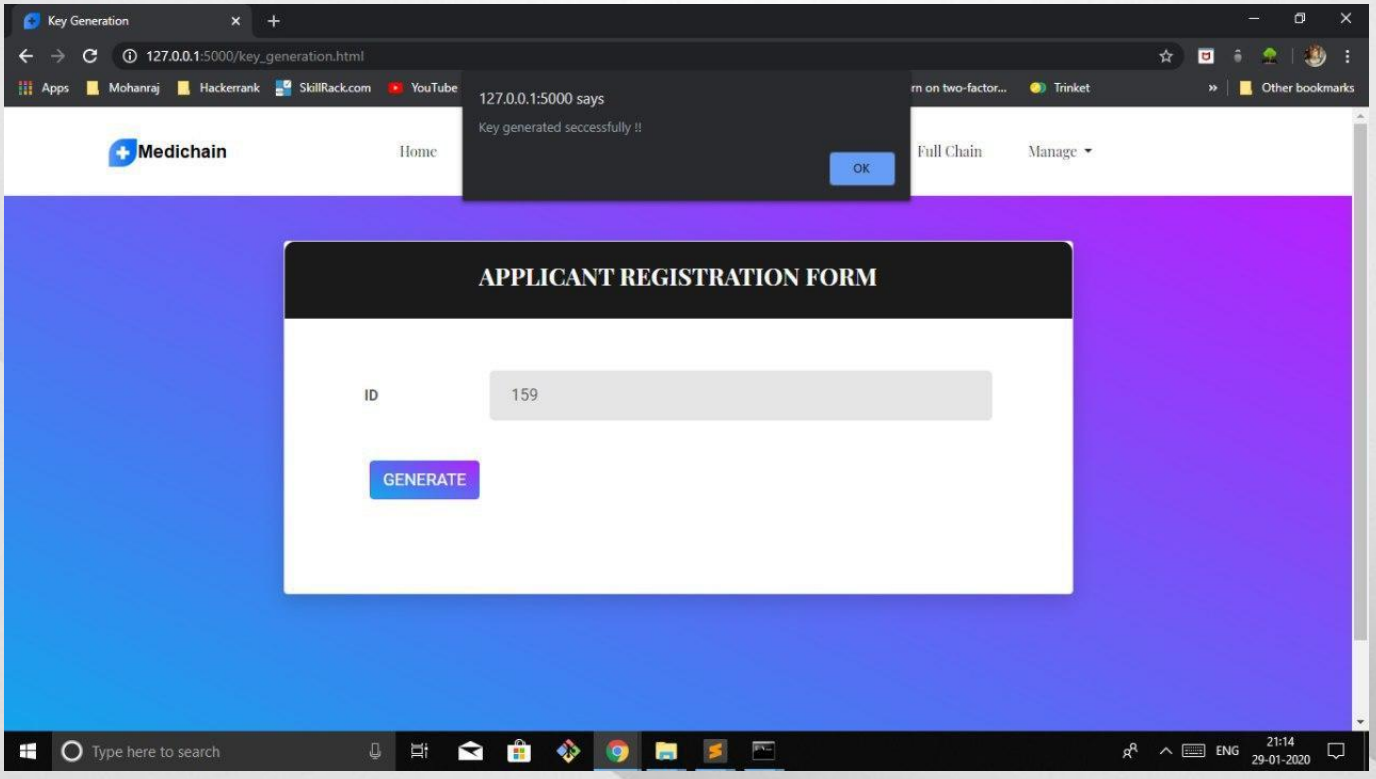
Background logs-4 (Hyperledger Fabric Deployment)

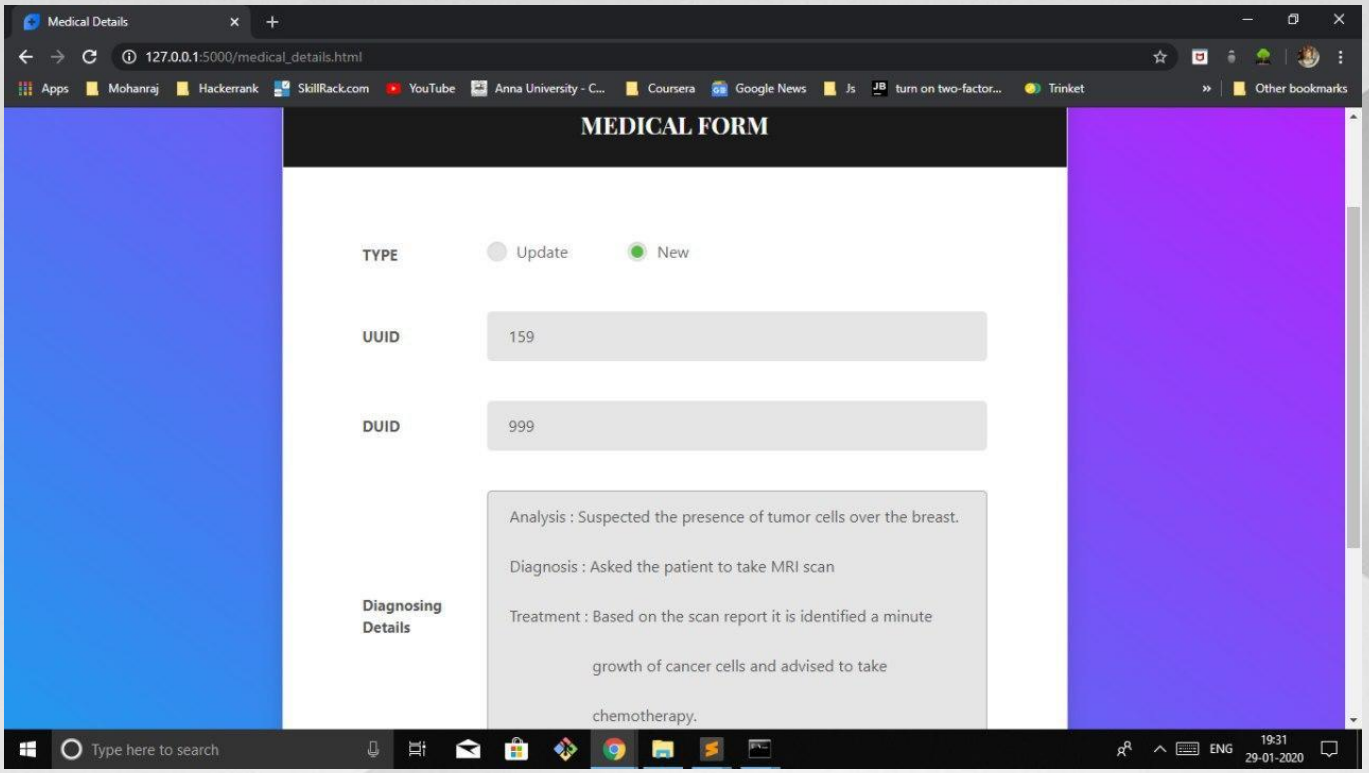


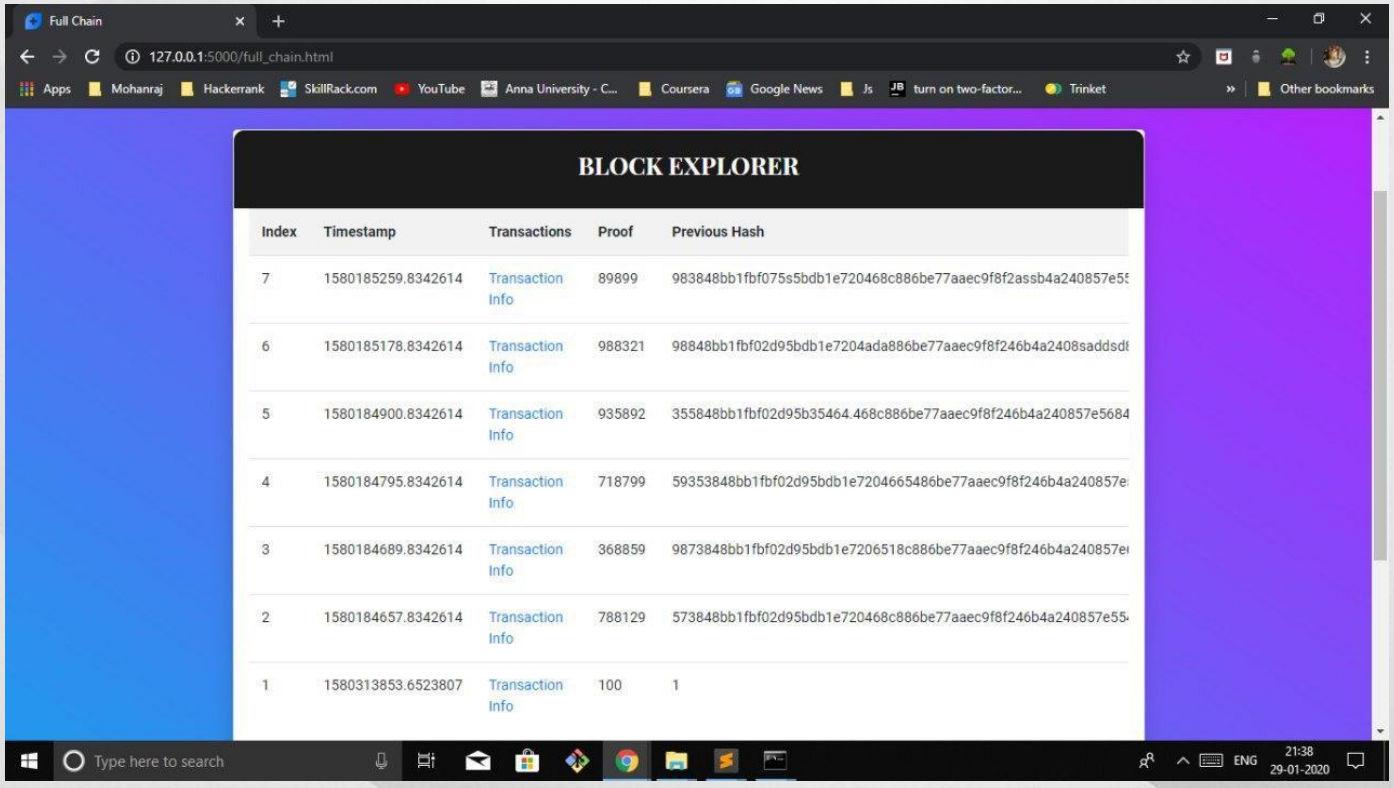
Background logs-5 (Fabric Chaincode installation and invocation)

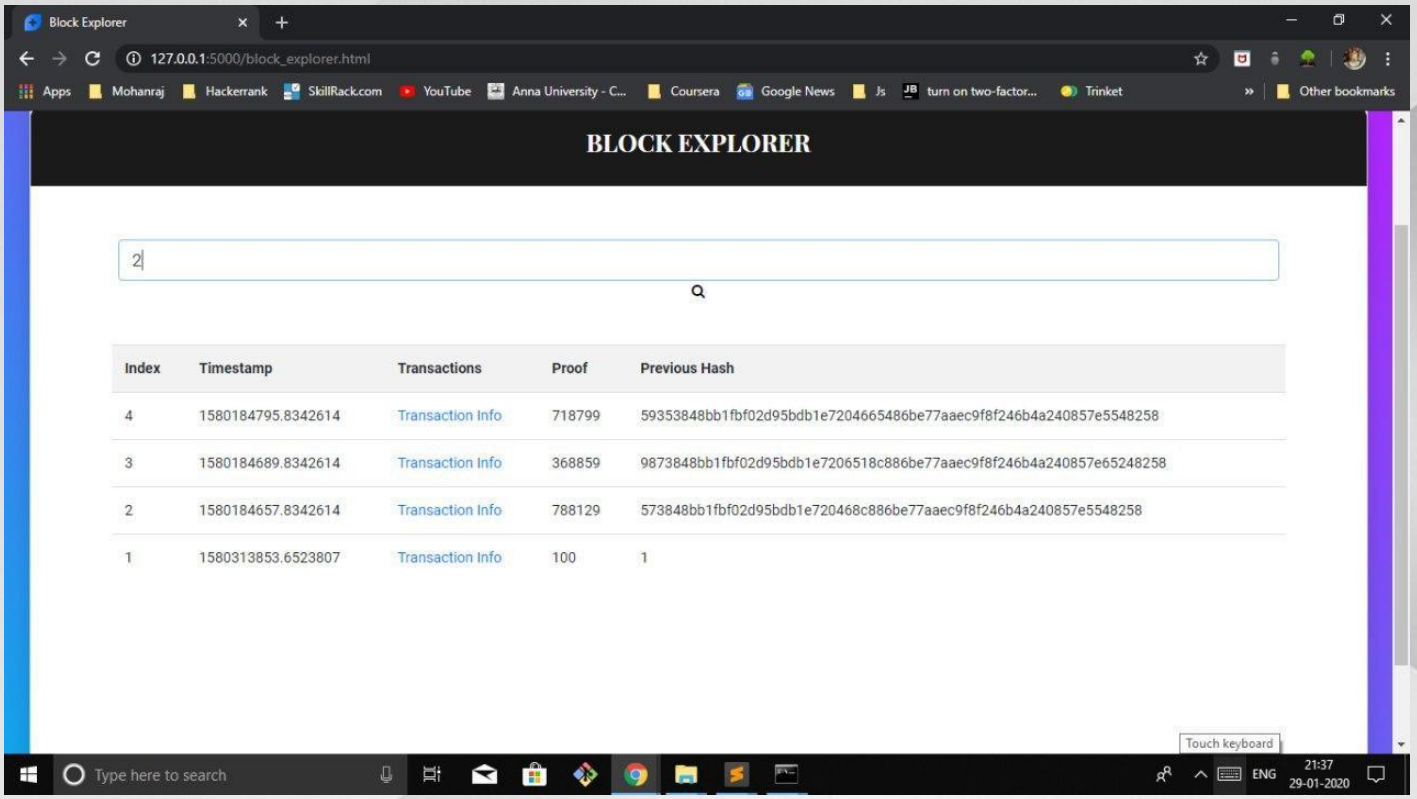
Frontend (WebApp):

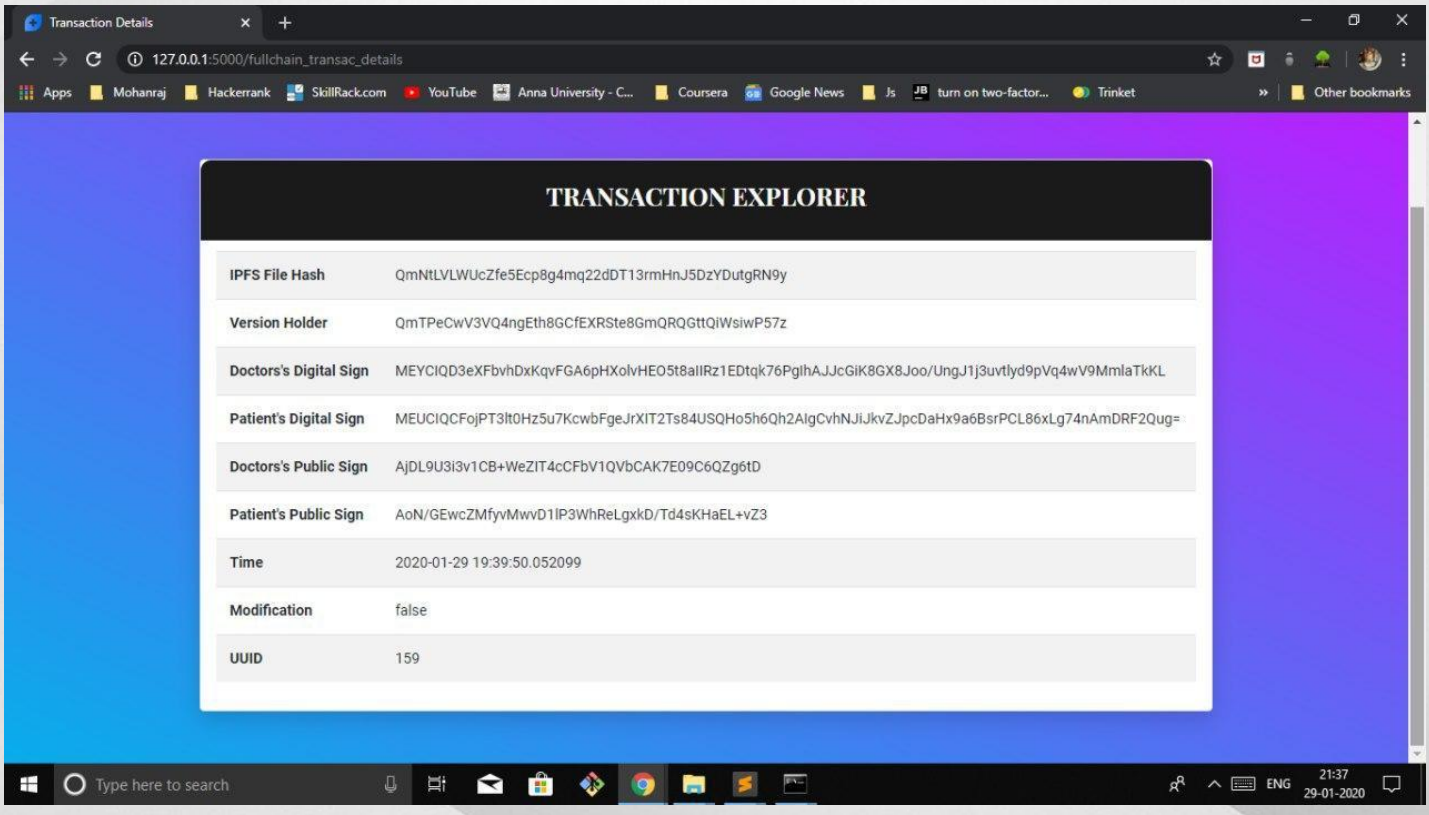


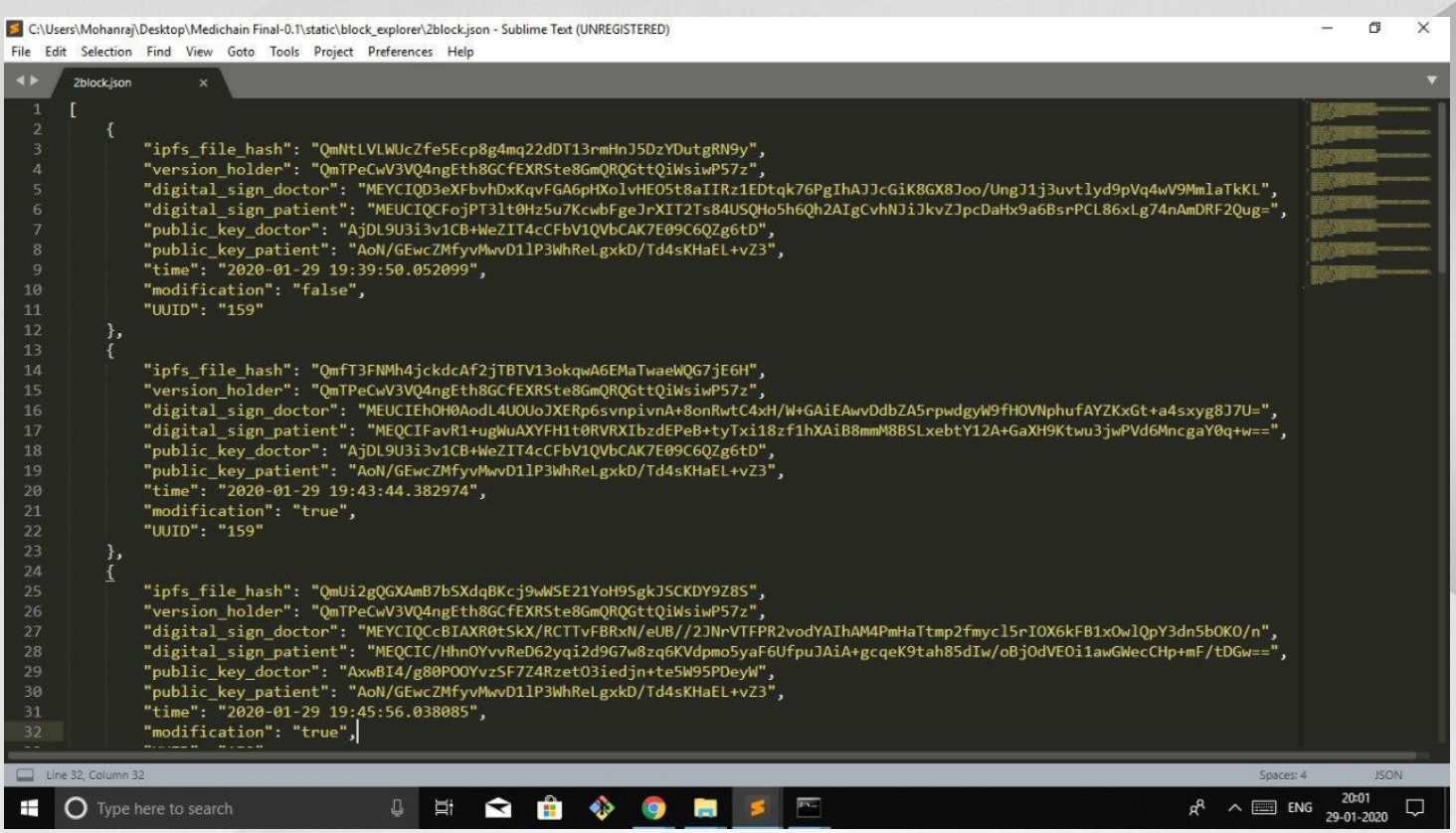


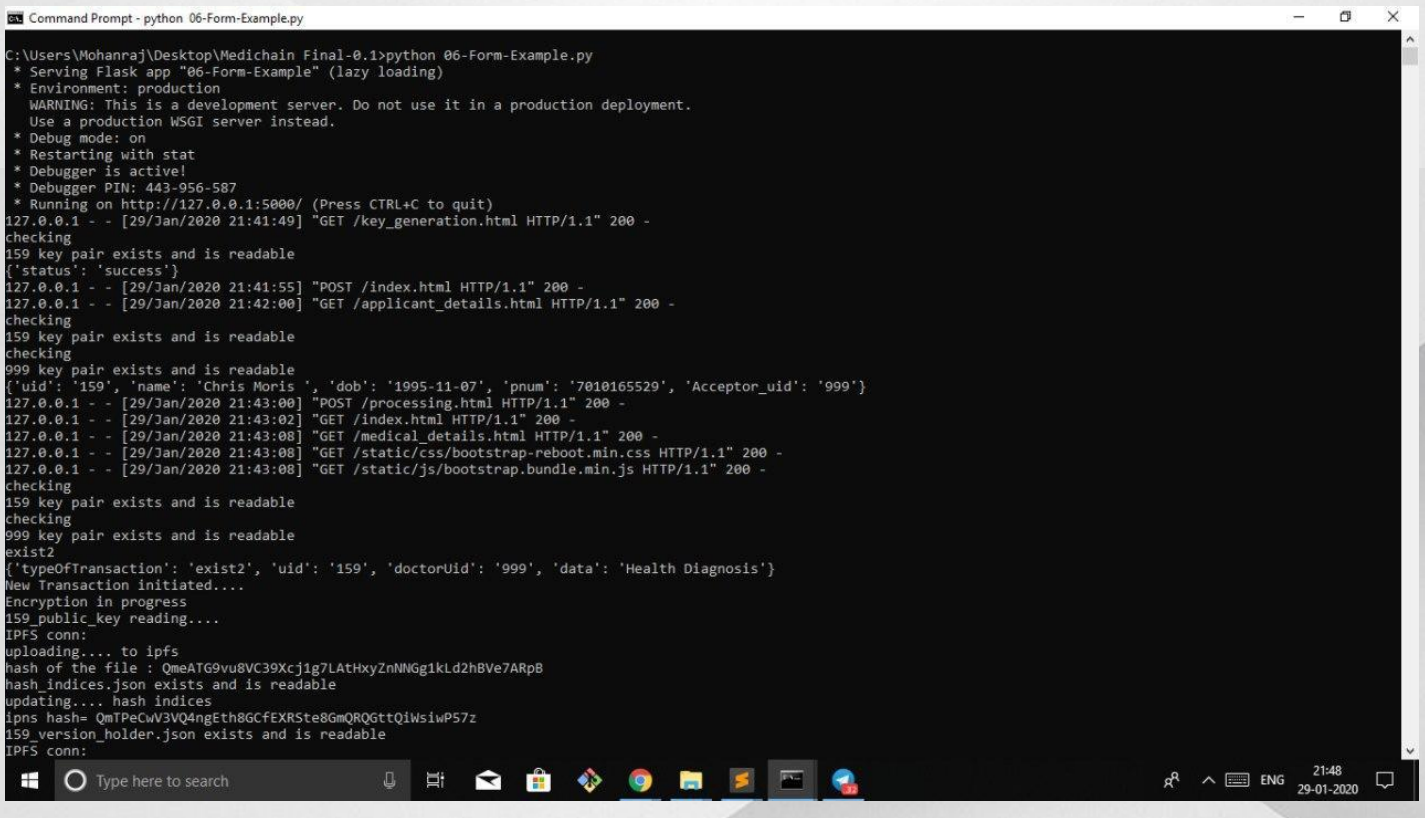

Medical Details
127.0.0.1:5000/medical_details.html
MEDICAL FORM
TYPE
Update
New
UUID
159
DUID
999
Diagnosing Details
Analysis : Suspected the presence of tumor cells over the breast.
Diagnosis : Asked the patient to take MRI scan
Treatment : Based on the scan report it is identified a minute growth of cancer cells and advised to take chemotherapy.

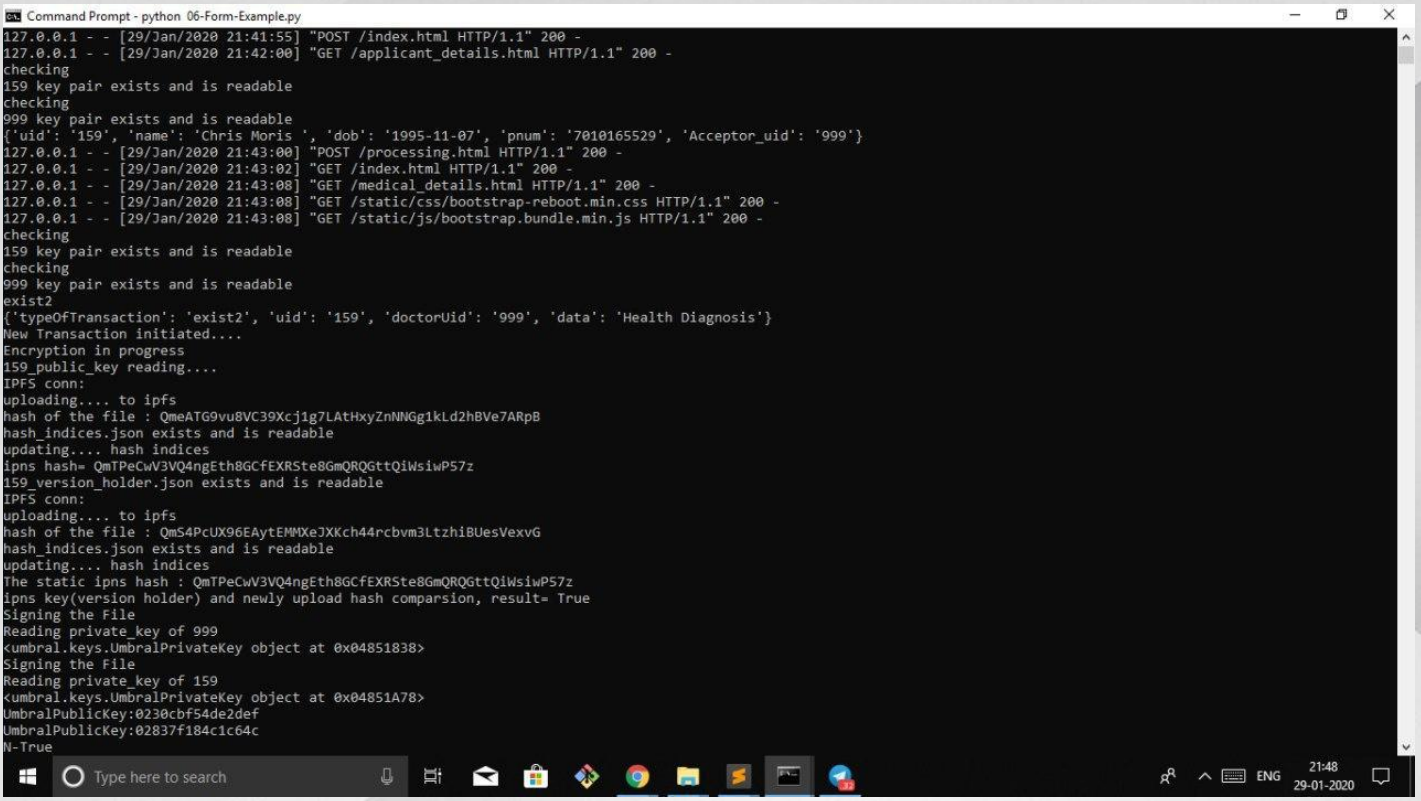

Full Chain
127.0.0.1:5000/full_chain.html
BLOCK EXPLORER
Index
Timestamp
Transactions
Proof
Previous Hash
7
1580185259.8342614
Transaction Info
89899
983848bb1fbf075s5bdb1e720468c886be77aaec9f8f2assb4a240857e5
6
1580185178.8342614
Transaction Info
988321
98848bb1fbf02d95bdb1e7204ada886be77aaec9f8f246b4a2408saddsd
5
1580184900.8342614
Transaction Info
935892
355848bb1fbf02d95b35464.468c886be77aaec9f8f246b4a240857e5684
4
1580184795.8342614
Transaction Info
718799
59353848bb1fbf02d95bdb1e7204665486be77aaec9f8f246b4a240857e
3
1580184689.8342614
Transaction Info
368859
9873848bb1fbf02d95bdb1e7206518c886be77aaec9f8f246b4a240857e
2
1580184657.8342614
Transaction Info
788129
573848bb1fbf02d95bdb1e720468c886be77aaec9f8f246b4a240857e55
1
1580313853.6523807
Transaction Info
100
1

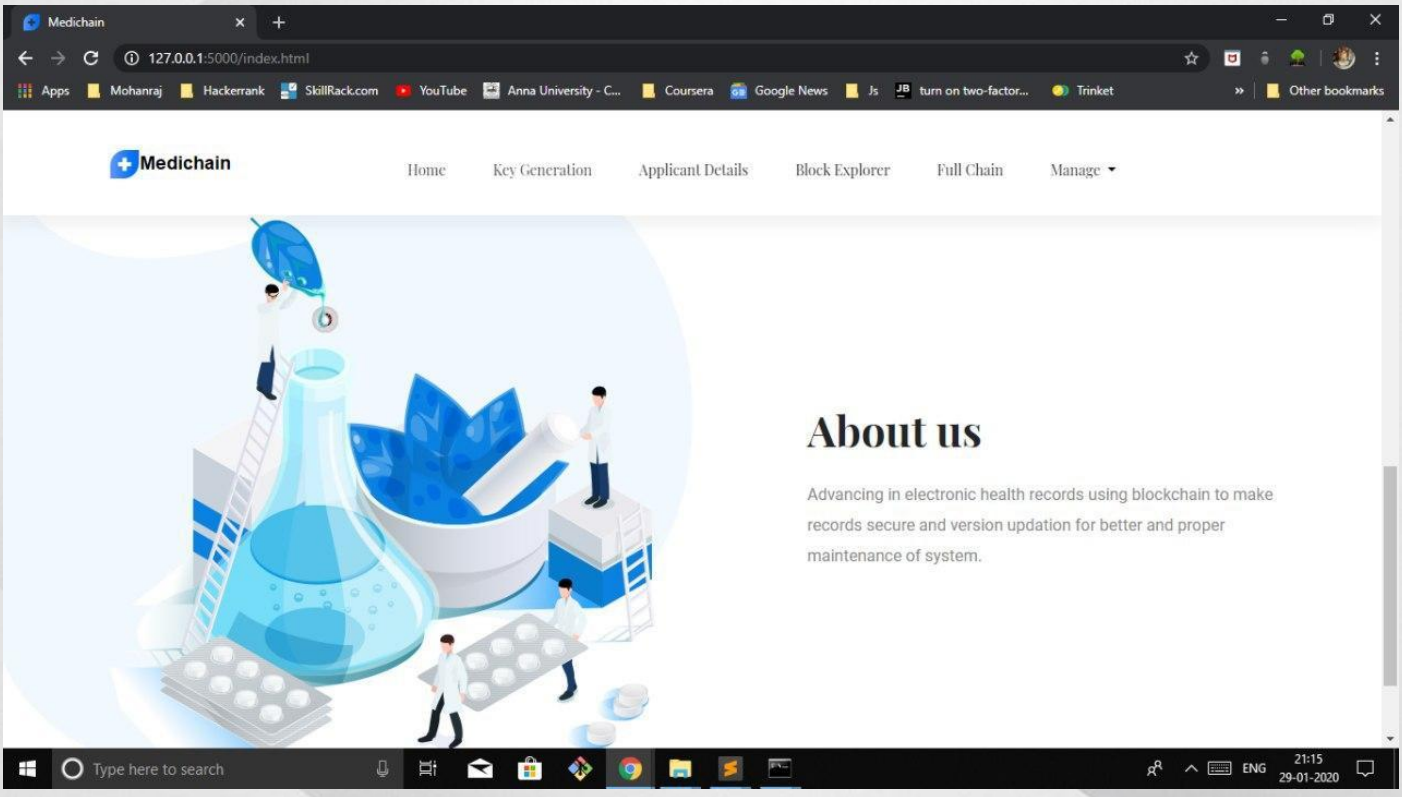

Block Explorer
127.0.0.1:5000/block_explorer.html
BLOCK EXPLORER
2
Index
Timestamp
Transactions
Proof
Previous Hash
4
1580184795.8342614
Transaction Info
718799
59353848bb1fbf02d95bdb1e7204665486be77aaec9f8f246b4a240857e5548258
3
1580184689.8342614
Transaction Info
368859
9873848bb1fbf02d95bdb1e7206518c886be77aaec9f8f246b4a240857e65248258
2
1580184657.8342614
Transaction Info
788129
573848bb1fbf02d95bdb1e720468c886be77aaec9f8f246b4a240857e5548258
1
1580313853.6523807
Transaction Info
100
1
Touch keyboard
Type here to search
ENG
21:37
29-01-2020


Transaction Details
127.0.0.1:5000/fullchain_transac_details
TRANSACTION EXPLORER
IPFS File Hash
QmNtLVLWUcZfe5Ecp8g4mq22dDT13rmHnJ5DzYDutgRN9y
Version Holder
QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z
Doctors's Digital Sign
MEYCIQD3eXFbvhDxKqvFGA6pHXolvHEO5t8aIIRz1EDtqk76PgIhAJJcGiK8GX8Joo/UngJ1j3uvtlyd9pVq4wV9MmlaTkKL
Patient's Digital Sign
MEUCIQCFojPT3lt0Hz5u7KcwbFgeJrXIT2Ts84USQHo5h6Qh2AlgCvhNJiJkvZJpcDaHx9a6BsrPCL86xLg74nAmDRF2Qug=
Doctors's Public Sign
AjDL9U3i3v1CB+WeZIT4cCFbV1QVbCAK7E09C6QZg6tD
Patient's Public Sign
AoN/GEwcZMfyvMwvD1lP3WhReLgxkD/Td4sKHaEL+vZ3
Time
2020-01-29 19:39:50.052099
Modification
false
UUID
159
Type here to search
ENG
21:37
29-01-2020


C:\Users\Mohanraj\Desktop\Medichain Final-0.1\static\block_explorer\2block.json - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
2block.json
[
{
"ipfs_file_hash": "QmNtLVLWUcZfe5Ecp8g4mq22dDT13rmHnJ5DzYDutgRN9y",
"version_holder": "QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z",
"digital_sign_doctor": "MEYCIQD3eXFbvhDxKqvFGA6pHXolvHEO5t8aIIRz1EDtqk76PgIhAJJcGiK8GX8Joo/UngJ1j3uvtlyd9pVq4wV9MmlaTkKL",
"digital_sign_patient": "MEUCIQCFojPT3lt0Hz5u7KcwbFgeJrXIT2Ts84USQHo5h6Qh2AIgCvhNJiJkvZJpcDaHx9a6BsrPCL86xLg74nAmDRF2Qug=",
"public_key_doctor": "AjDL9U3i3v1CB+WeZIT4cCFbV1QVbCAK7E09C6QZg6tD",
"public_key_patient": "AoN/GEwcZMfyvMwvD1lP3WhReLgxkD/Td4sKHaEL+vZ3",
"time": "2020-01-29 19:39:50.052099",
"modification": "false",
"UUID": "159"
},
{
"ipfs_file_hash": "QmfT3FNMh4jckdcAf2jTBTV13okqwA6EMaTwaeWQG7jE6H",
"version_holder": "QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z",
"digital_sign_doctor": "MEUCIEhOH0AodL4UOUoJXERp6svnpivnA+8onRwtC4xH/W+GAiEAwvDdbZA5rpwdgyW9fHOVNphufAYZKxGt+a4sxyg8J7U=",
"digital_sign_patient": "MEQCIFavR1+ugWuAXYFH1t0RVRXIbzdEPeB+tyTxi18zf1hXAiB8mmM8BSLxebtY12A+GaXH9Ktwu3jwPVd6MncgaY0q+w==",
"public_key_doctor": "AjDL9U3i3v1CB+WeZIT4cCFbV1QVbCAK7E09C6QZg6tD",
"public_key_patient": "AoN/GEwcZMfyvMwvD1lP3WhReLgxkD/Td4sKHaEL+vZ3",
"time": "2020-01-29 19:43:44.382974",
"modification": "true",
"UUID": "159"
},
{
"ipfs_file_hash": "QmUi2gQGXAmB7bSXdqBKcj9wWSE21YoH9SgkJSCKDY9Z8S",
"version_holder": "QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z",
"digital_sign_doctor": "MEYCIQCcBIAXR0tSkX/RCTTvFBRxN/eUB//2JNrVTFPR2vodYAIhAM4PmHaTtmp2fmycl5rIOX6kFB1xOwlQpY3dn5bOKO/n",
"digital_sign_patient": "MEQCIC/HhnOYvvReD62yqi2d9G7w8zq6KVdpmo5yaF6UfpuJAiA+gcqeK9tah85dIw/oBjOdVEOi1awGWecCHp+mF/tDGw==",
"public_key_doctor": "AxwBI4/g80POOYvzSF7Z4RzetO3iedjn+teSW95PDeyW",
"public_key_patient": "AoN/GEwcZMfyvMwvD1lP3WhReLgxkD/Td4sKHaEL+vZ3",
"time": "2020-01-29 19:45:56.038085",
"modification": "true",
Line 32, Column 32
Spaces: 4
JSON
Type here to search
ENG
20:01
29-01-2020


Command Prompt - python 06-Form-Example.py
C:\Users\Mohanraj\Desktop\Medichain Final-0.1>python 06-Form-Example.py
* Serving Flask app "06-Form-Example" (lazy loading)
* Environment: production
WARNING: This is a development server. Do not use it in a production deployment.
Use a production WSGI server instead.
* Debug mode: on
* Restarting with stat
* Debugger is active!
* Debugger PIN: 443-956-587
* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [29/Jan/2020 21:41:49] "GET /key_generation.html HTTP/1.1" 200 -
checking
159 key pair exists and is readable
{'status': 'success'}
127.0.0.1 - - [29/Jan/2020 21:41:55] "POST /index.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:42:00] "GET /applicant_details.html HTTP/1.1" 200 -
checking
159 key pair exists and is readable
checking
999 key pair exists and is readable
{'uid': '159', 'name': 'Chris Moris ', 'dob': '1995-11-07', 'pnum': '7010165529', 'Acceptor_uid': '999'}
127.0.0.1 - - [29/Jan/2020 21:43:00] "POST /processing.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:02] "GET /index.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /medical_details.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /static/css/bootstrap-reboot.min.css HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /static/js/bootstrap.bundle.min.js HTTP/1.1" 200 -
checking
159 key pair exists and is readable
checking
999 key pair exists and is readable
exist2
{'typeOfTransaction': 'exist2', 'uid': '159', 'doctorUid': '999', 'data': 'Health Diagnosis'}
New Transaction initiated....
Encryption in progress
159_public_key reading....
IPFS conn:
uploading.... to ipfs
hash of the file : QmeATG9vu8VC39Xcj1g7LAtHxyZnNNGg1kLd2hBVe7ARpB
hash_indices.json exists and is readable
updating.... hash indices
ipns hash= QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z
159_version_holder.json exists and is readable
IPFS conn:
Type here to search
ENG
21:48
29-01-2020


Command Prompt - python 06-Form-Example.py
127.0.0.1 - - [29/Jan/2020 21:41:55] "POST /index.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:42:00] "GET /applicant_details.html HTTP/1.1" 200 -
checking
159 key pair exists and is readable
checking
999 key pair exists and is readable
{'uid': '159', 'name': 'Chris Moris ', 'dob': '1995-11-07', 'pnum': '7010165529', 'Acceptor_uid': '999'}
127.0.0.1 - - [29/Jan/2020 21:43:00] "POST /processing.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:02] "GET /index.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /medical_details.html HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /static/css/bootstrap-reboot.min.css HTTP/1.1" 200 -
127.0.0.1 - - [29/Jan/2020 21:43:08] "GET /static/js/bootstrap.bundle.min.js HTTP/1.1" 200 -
checking
159 key pair exists and is readable
checking
999 key pair exists and is readable
exist2
{'typeOfTransaction': 'exist2', 'uid': '159', 'doctorUid': '999', 'data': 'Health Diagnosis'}
New Transaction initiated....
Encryption in progress
159_public_key reading....
IPFS conn:
uploading.... to ipfs
hash of the file : QmeATG9vu8VC39Xcj1g7LAtHxyZnNNGg1kLd2hBVe7ARpB
hash_indices.json exists and is readable
updating.... hash indices
ipns hash= QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z
159_version_holder.json exists and is readable
IPFS conn:
uploading.... to ipfs
hash of the file : QmS4PcUX96EAytEMMXeJXKch44rcbvm3LtzhiBUesVexvG
hash_indices.json exists and is readable
updating.... hash indices
The static ipns hash : QmTPeCwV3VQ4ngEth8GCfEXRSte8GmQRQGttQiWsiwP57z
ipns key(version holder) and newly upload hash comparsion, result= True
Signing the File
Reading private_key of 999
<umbral.keys.UmbralPrivateKey object at 0x04851838>
Signing the File
Reading private_key of 159
<umbral.keys.UmbralPrivateKey object at 0x04851A78>
UmbralPublicKey:0230cbf54de2def
UmbralPublicKey:02837f184c1c64c
N-True
Type here to search
ENG
21:48
29-01-2020


Medichain
127.0.0.1:5000/index.html
Apps
Mohanraj
Hackerrank
SkillRack.com
YouTube
Anna University - C...
Coursera
Google News
Js
turn on two-factor...
Trinket
Other bookmarks
Medichain
Home
Key Generation
Applicant Details
Block Explorer
Full Chain
Manage
About us
Advancing in electronic health records using blockchain to make records secure and version updation for better and proper maintenance of system.
Type here to search
ENG
21:15
29-01-2020