

2018/09/01

Considering a group of 5 people (X1, X2, X3, X4, X5), X1 wants to share a file (F1) with others. X1 will apply secret sharing scheme on F1 and create 5 shares (S1, S2, S3, S4, S5). These shares are uploaded in IPFS. The hash generated by IPFS will be given to the group. Each individual of the group will maintain a chain that stores hash of the share along with the file ID.

Workflow

- Split the file into shares
- Add shares to IPFS
- Update the chain
- Retrieve on demand basis

Split the file into shares

- By applying the secret sharing scheme (1,3,5) [where file is divided into 5 shares, among 3 is required to regenerate the file]
- One among the share is essential
 - Should not be viewed by anyone except the owner
 - Reveal on demand
- Other shares can be viewed by anyone

Add shares to IPFS

Updation of chain

Each X_i will update the chain with the file ID and IPFS hash of S_i

Retrieve On demand basis

- When some nodes want to recreate the file the shares need to be recombined with essential share

Queries:

- Is the path traceable using DHT? (as DHT stores the pointer to the node that stores digital object). If it is traceable, attack (Content reveal) is possible
- When the node Pinned the digital objects, Unpinned the same, will the content be still available? (.....because in IPFS the data lives forever)

Work Done

Step 1: Installed IPFS in two Systems (consider as node A and Node B) that were in same subnet (Intranet)

Step 2: Initiated Daemon – Viewed

- Peer ID
- Public Key
- Private Key

```
please run: 'ipfs init'
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs init
initializing IPFS node at /home/mariya/.ipfs
generating 2048-bit RSA keypair...done
peer identity: QmP6uhT1DQNWurADieYJJJo58HgmaAsWo5Y33Mr173t8Wso
to get started, enter:

ipfs cat /ipfs/QmS4ustL54uo8FzR9455qaxZwuMiUhyvMcX9Ba8nUH4uVv/readme
```

- Exported the IPFS to different path and viewed
- Modification Observed in above all 3 parameters

```
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ export IPFS_PATH="/home/mariya/one/a"
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs init
initializing IPFS node at /home/mariya/one/a
generating 2048-bit RSA keypair...done
peer identity: QmQPTC3bBX1Ja9VJ8ZE7yhNJYrW4BoNq2pCf9eLiaTPEFC
to get started, enter:

ipfs cat /ipfs/QmS4ustL54uo8FzR9455qaxZwuMiUhyvMcX9Ba8nUH4uVv/readme

mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ export IPFS_PATH="/home/mariya/one/b"
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs id
Error: no IPFS repo found in /home/mariya/one/b.
please run: 'ipfs init'
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$
```

- When a new terminal is opened and **IPFS id** is given it will display the **initial ID**

Please use
ctrl+paste
of text not
finger.

```
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs init
initializing IPFS node at /home/mariya/one/b
generating 2048-bit RSA keypair...done
peer identity: QmQPnhhEU3RHNC2w7fx99S2tJnQU4TqiVAvtovdn1LXh16
to get started, enter:

    ipfs cat /ipfs/QmS4ustL54uo8FzR9455qaxZwuMiUhyvMcX9Ba8nUH4uVv/readme

mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs id
{
  "ID": "QmQPnhhEU3RHNC2w7fx99S2tJnQU4TqiVAvtovdn1LXh16",
  "PublicKey": "CAASpgIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7TxhbVdItYzrAeFPh+TtPqZN2VJpV00zIPKn3CmC+wUKzL0aEqYspYrk990zS/GyoAnz1UhbDpL0FRSHbUwn1Qzk22Xg1/GjBjWfIgdM17o4Y5goucYz1ICzoCRfEAItM6Z660UocquG6iaydYPTjYyI7kjhCLAMPmioV5hzSBn2GZNpeGVJ98kz+uZURQqve3TquYIm86fa0pgpXSscQvsSDNjSkQVn7uDBvpAWmvYpId+Td1ScimgrI2TN5sYJB+k1YeCHSW12LoFvHswKXiAEONyBVYzUf7IYAGSue1f2b1vDeNLIIs3ZXyODLSAlrXTd0ojGst8Ual7B9T5KZhAgMBAAE=",
  "Addresses": null,
  "AgentVersion": "go-ipfs/0.4.17/",
  "ProtocolVersion": "ipfs/0.1.0"
}

mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$
```

```
mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$ ipfs id
{
  "ID": "QmP6uhT1DQNWurADieYJJo58HgmAsWo5Y33Mr173t8Wso",
  "PublicKey": "CAASpgIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7TxhbVdItYzrAeFPh+TtPqZN2VJpV00zIPKn3CmC+wUKzL0aEqYspYrk990zS/GyoAnz1UhbDpL0FRSHbUwn1Qzk22Xg1/GjBjWfIgdM17o4Y5goucYz1ICzoCRfEAItM6Z660UocquG6iaydYPTjYyI7kjhCLAMPmioV5hzSBn2GZNpeGVJ98kz+uZURQqve3TquYIm86fa0pgpXSscQvsSDNjSkQVn7uDBvpAWmvYpId+Td1ScimgrI2TN5sYJB+k1YeCHSW12LoFvHswKXiAEONyBVYzUf7IYAGSue1f2b1vDeNLIIs3ZXyODLSAlrXTd0ojGst8Ual7B9T5KZhAgMBAAE=",
  "Addresses": null,
  "AgentVersion": "go-ipfs/0.4.17/",
  "ProtocolVersion": "ipfs/0.1.0"
}

mariya@mariya-HP-Pro-3090-MT:~/one/go-ipfs$
```

Query 1: Is the peer ID is unique

Yes, Peer ID is unique for the system/ Node. Though multiple export action performed finally when we tried to retrieve IPFS ID, the initial value is displayed (peer id generated at the time of initial installation)

Query 2: Replace the config file and verify the peer ID is over written or not

Did you do this?

Step 3: Added files to IPFS and viewed

- once a file is added, hash is generated and displayed
- Hash is used for retrieving


```

kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ echo "123456789" > sample_1.txt
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ clear

kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ echo "123456789" > sample_1.txt
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ cat sample_1.txt
123456789
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ echo "abcdefghijklmnopqrstuvwxy
z" > sample_2.txt
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ cat sample_2.txt abcdefghijklmn
opqrstuvwxyz
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ls
sample_1.txt  sample_2.txt
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ipfs add sample_1.txt
added QmRXdTZ4dQR2b95B9nBgr5efTveqFlxvv72xMqDCV4NM4h sample_1.txt
10 B / 10 B [=====] 100.00%kalpanak
umar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ipfs add sample_2.txt
added Qmancr1PHuFLrhUEuU75ffxCiBDNGZm5V1jam9iXZY479V sample_2.txt
27 B / 27 B [=====] 100.00%kalpanak
umar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ipfs cat QmRXdTZ4dQR2b95B9nBgr5efTveqFi
xvv72xMqDCV4NM4h
123456789
kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ipfs add sample_2.txt
added Qmancr1PHuFLrhUEuU75ffxCiBDNGZm5V1jam9iXZY479V sample_2.txt
27 B / 27 B [=====] 100.00%kalpanak

```

•Pin (recursive and indirect) and Unpin the file

```

kalpanakumar@kalpanakumar-Precision-WorkStation-T5500:~/IPFS_Sample_File$ ipfs pin ls
QmZTR5bcpQD7cFgTorqxZDYaew1Wqgfbd2ud9QqGPAkK2V indirect
QmY5heUM5qgRubMDD1og9fhCPA6QdkMp3QCwd4s7gJsyE7 indirect
QmejvEPop4D7YUadeGqYwMZXhHLC4JBUCzJJHWMzdcMe2y indirect
QmXgqKTbzdh83pQtKfb19SpMCpDDcKR2ujqk3pKph9aCNF indirect
QmPZ9gcCEepKTo6aq61g2nXGUhM4iCL3ewB6LDXZCtioEB indirect
QmS4ustL54uo8FzR9455qaxZwuMiUhyvMcX9Ba8nUH4uVv recursive
Qmancr1PHuFLrhUEuU75ffxCiBDNGZm5V1jam9iXZY479V recursive
QmQ5vhrL7uv6tuoN9KeVBwd4PwfQkXdVvMDLUZuTNxqgvM indirect
QmYCvbfNbCwFR45HiNP45rwJgvatpiW38D961L5qAhUM5Y indirect
QmUNLLsPACcz1vLxQVqXqQLX5R1X345qqfHbsf67hvA3Nn recursive
QmRXdTZ4dQR2b95B9nBgr5efTveqFlxvv72xMqDCV4NM4h recursive

```

Query 3: When a node is down/ disconnected from network, will be able to get the content pinned by that node?

Yes, it is possible to retrieve the content