# Blockchain Based Identity Verification Model

Gunit Malik
*B.Tech Computer Engineering*
*NMIMS, MPSTME*
Mumbai Campus, India
gunit.tdk@gmail.com

Kshitij Parasrampuria
*B.Tech Computer Engineering*
*NMIMS, MPSTME*
Mumbai Campus, India
kp.puria@gmail.com

Sai Prasanth Reddy
*B.Tech Computer Engineering*
*NMIMS, MPSTME*
Mumbai Campus, India
saiprasanthreddy4@gmail.com

Dr. Seema Shah
*Faculty*
*NMIMS, MPSTME*
Mumbai Campus, India
seema.shah@nmims.edu

***Abstract*—Blockchain is peer-to-peer decentralized system that provides security, reliability, authenticity, immutability and transparency. It is an expandable list of records called blocks which are linked using cryptography. Blockchain by design, is resilient to modifications, it consists of an open distributed ledger that records all the transactions made between two parties which cannot be forged. This paper provides a unique model for document verification with use case of the government. Currently all issuing authorities are separate cells providing identity documents to a citizen. Due to this cellular nature document verification is a tedious and long process. The problem of falsifying documents is another issue within government bodies. We discuss the use of Blockchain to improve efficiency and security. The purpose of this project is to develop a private permissioned blockchain network where an individuals official documents can be shared by government bodies, organizations and educational institutions. Using the Blockchain technology, our platform achieves a decentralized system to share authenticated government documents between government bodies and private organizations without the need of a certain level of human intervention. With the concluding facts of this paper, it is observed that the process of document verification and issuing process's efficiency is drastically improved with our blockchain model. Along with this we reap benefits of security, reliability and transparency.**

***Index Terms*—IPFS, Block, Node, Blockchain, Hyperledger, Document Verification, Smart Contracts, Asymmetric Encryption.**

## I. Introduction

Blockchain was first introduced in 2008 by Satoshi Nakamoto. It was the founding technology initially used in Bitcoin, a digital currency. Blockchain has since seeped its way into various domains [1] [2] [3] [4] proving its usefulness across the board. Blockchain is a decentralised peer based network, where each peer, also called a node stores information about all the transactional records of the network. Every transaction is linked to the previous transaction on the chain, and before being stored needs consensus from more than half the nodes on the chain. Hence, the trust, immutability and security is high as changing any block of the chain would need previous blocks to be changed too, which is not very feasible to attackers. [5] [6] [7]

India has a population of 1.34 Billion. With a population that high, the process of issuing and verifying the identification documents(Passport, Adhaar Card, PAN Card, Voters ID, etc) of each and every citizen must be reliable, secure and quick. The current systems in place are functional, but the efficiency and security needs to be improved as the process usually takes several weeks and the citizens applying for the documents may have to visit the issuing authority offices multiple times to get documents successfully. This is not only inconvenient and time consuming but also monetarily and environmentally expensive.

In this paper, we have discussed a blockchain based solution for verifying the authenticity of the documents issued by the Indian Government authorities. The advantage of using this system is that it provides a quick, reliable and secure channel [8] for issuing authorities to access documents of an individual who has other documents directly from the databases of the other issuing authorities. This access is permissioned and time bounded, so privacy concerns are eliminated.

The paper is structured as follows. In Section[II], we introduce the structure and architecture of blockchain along with the elements that constitute the blockchain technology. In Section[III], we describe the current state of the verification process in government institutions and which issues can be resolved. In Section[IV], we provide a description of the proposed model in terms of design, implementation and discussion. Lastly, we conclude our findings based on our implemented model.

## II. Blockchain Structure

### *A. Block*

It is a compilation of predefined number of transactions that occur in the blockchain. Each block has a unique identification.

### *B. Chain*

It is the element that links two blocks in a blockchain. A hash is calculated using hashing algorithms like SHA1 or SHA2, which use data existing in the previous block to generate the hash value [9]. The linking is done by the generation of hash. The hash is called a chain.

### *C. Node*

Nodes are the storage data centers of the blockchain. The transactions on the blockchain are verified and added to the chain by the verified nodes. A node can be any kind of a device (a computer, a laptop, a server, etc.) depending on

978-1-5386-9353-7/19/$31.00 ©2019 IEEE

the requirements of the chain. Each verified node has the transaction history of the entire chain. Thus, theoretically, the blockchain resides on every node. Nodes perform the following functions:

- Accept or reject transactions based on their validity.
- Store records of all the transactions that happen.
- Broadcast valid transactions throughout the chain for other nodes to synchronize with the blockchain.

### D. Network

It is the collection of all the nodes connected by chains, and all the other. A network is the home to all the other elements of the blockchain.

### E. Smart Contract

It is a piece of code that runs on a blockchain. It works as a non-repudiation agent, meaning that it locks both the parties in every transaction so ownership can't be denied.

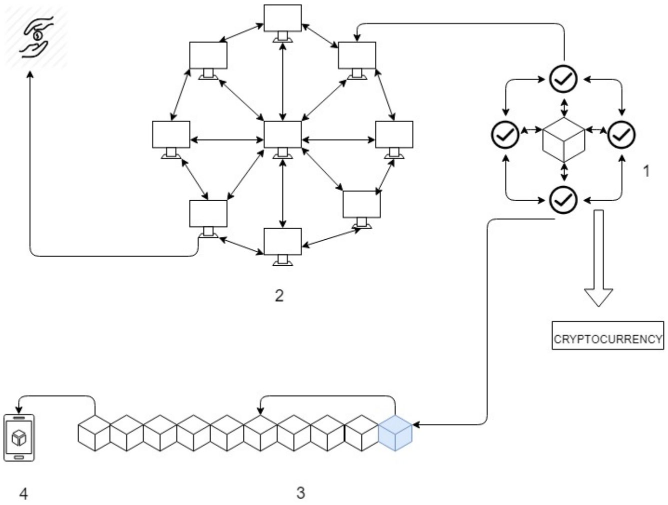


Fig. 1. Blockchain Structure Overview

Fig. 1 shows the overview of the blockchain structure with the following process flow:

1) When a transaction is requested by a node, it is propagated to the other nodes for approval. An approved transaction can involve cryptocurrency, contracts, records or other information.
2) Shows how a transaction is propagated to multiple nodes by the requesting node. The transaction is verified by the other nodes on the chain using a predefined set of algorithms. Smart Contracts are programs that can be run on the blockchain network as an added feature which ensure non-repudiation [10].
3) When a block reaches its transaction limit, it is added to the chain and is then immutable.
4) The transaction process ends with the addition of the block to the chain.

## III. Current State of the Verification Process

For application of new documents, eg. Aadhaar, Passport, Driver's License etc. there are pre-requisite documents that need to be submitted to the issuing authorities (for proof of address and so on). Once the documents have been submitted, the issuing authorities must then go through the process of verification of these documents to validate their authenticity and validity. This process is done to avoid fraudulent activity and ensure that the information provided is valid.

The issuing authority of the document assigns a team to conduct this verification process by contacting the issuing authority of the document that has to be verified. The process has the following problems:

- It is time consuming
- Tedious for both the applicant and the issuing authority
- Delays in the verification are caused due to human error
- Expensive as multiple agents are involved

To overcome these problems in the current system, a new platform can be developed, which is:

- Centralized
- Secure
- Quick
- Reliable

This new system is blockchain based and solves the problems of the current system as explained in section[IV] implementation.

TABLE I
Market Survey Of Aligned Projects

| ***Application*** | ***Type of blockchain*** | ***Certificates supported*** |
|---|---|---|
| BCertx | Bitcoin Blockchain | Academic certificates |
| Blockcerts | Bitcoin blockchain | Academic credentials, professional certifications, workforce development, and civic records |
| Blockpass | Ethereum Public Blockchain | Verification of humans (KYC), objects (KYO) and connected devices (KYD). Documents may or may not be retained. |
| Stampery | Bitcoin and Ethereum blockchains | All Documents Enterprises provide the list of documents. |
| CredyCo | Bitcoin blockchain | All Documents Enterprises provide the list of documents. |
| ExistenceID | Blockchain (not Storage) | Identity documents. |

Table 1. contains the market survey of the current organizations and projects that use blockchain technology for document verification. It can be observed that there is no such project that provides identity verification along with storage solution. Also majority projects use the concept of cryptocurrency which is not a requirement for the process of document verification, while also increasing the computing power required by the entire network.

## IV. Implementation

Blockchain is a combination of already existing technologies. It enables a decentralized, immutable and distributed ledger that can be used in countless use cases [11]. In this case, it provides a platform to the issuing authorities to verify authenticity of the submitted documents through a quick, reliable and secure channel. This will speed up the issuing of new documents drastically as the need to obtain documents from other issuing authorities and get them attested will be negated. Instead, all the original documents will be available through the blockchain itself.

When first introduced blockchains were public in nature. It was a system made up of peers who contribute due to incentives ie cryptocurrency like Bitcoin. Contrary to this private permisioned blockchains are made based on the authority of trusted peers. The blockchain's access control is managed by these peers thus providing a lower run complexity. With this type of blockchain network data is secure due to blockchain architecture and as well as transperency can be provided to individuals by virtue of immutable records. With private blockchains we have the advantages of:

- Private blockchains are more efficient: only trusted peers, with high processing power, are used to verify transactions.
- Network infrastructure can be planned and controlled. Various network-related problems (such as network delays and connection losses) might be faster to fix.
- If permissions are restricted, private blockchains can provide a greater level of privacy. [6]

### A. *Design*

Fig. 2 shows the model architecture of blockchain.

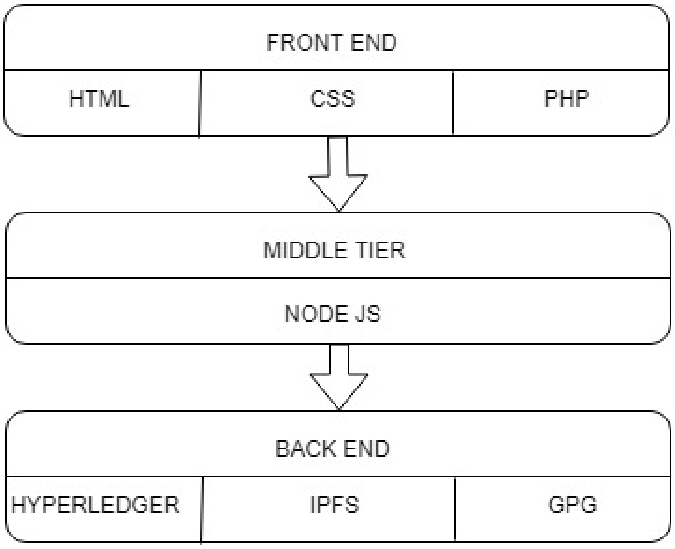


Fig. 2. Blockchain Model Architecture

*1) Platform: Hyperledger:* Hyperledger is an open-source permissioned blockchain system that is used by enterprises to share confidential information [12]. It promotes a wide range of blockchain technologies for businesses, finance and Internet of Things. These technologies include smart contracts, distributed ledgers, client libraries, graphical interfaces. Hyperledger Fabric is a platform with a modular architecture that delivers high degrees of confidentiality, flexibility and scalability for distributed ledgers.

It has many key properties, one such property is the support for smart contracts. Maintaining of the nodes(members) of the blockchain is done using MSP( Membership Service Providers).This allows the nodes to be known to each other. Fabric uses smart contracts called "chaincode" that form the logic of the system. This is done using the GO programming language.

Hyperledger Fabric as mentioned, is a permissioned blockchain that reveals the identity of each node in the system to one another. Every node added to the chain needs to be authenticated for the participation and transaction in the chain.This allows the nodes to know who is accessing particular data.

It also allows for access control over the participants to a certain level by restricting some of the privileges provided. The use of permissioned blockchain in verification of documents helps handle the high transaction rates and enhances performance.

Availability of channels help achieve privacy of certain data through data partitioning on the blockchain. Partitioning also allows members to be part of multiple private blockchains and choose to share/reference some of the data from a different blockchain.

*2) Interface:* The interface will be designed with HTML and CSS for the different issuing authorities. The authorized parties will be able to obtain access to the blockchain using this interface and will be able to verify the authenticity of the documents. The document holder will share a public key (given to him by the issuing authority) with the authority which wants to verify the authenticity of the documents. This key will allow the authority to access the document of the holder directly from the database of the issuing authority which will reduce the time consumed for verification. Using the key, the issuing authority can easily identify whether the document is legal or not.

*3) File Handling/ Database:* Blockchain has the ability to store small amounts of data in the blocks. However, the proof of work consensus mechanisms have slowed the transaction speeds to extremely low levels. Calculation and verification of the hash values to maintain integrity in the blockchain causes the storage of large files a nightmare.

Small data such as transaction details of bitcoin or other cryptocurrencies maybe stored in the blockchain but rich data such as large files and documents can be barely sustained. Moreover, according to the yellow paper, the fee for a 256-bit word is 20000 Gas (Gas is term introduced by Ethereum to calculate the amount of work done in a transaction). This data storage and transfer technique is not feasible in this case as documents can range over several kB. Documents provided by the government need to be stored and transferred between the institutions in fast and cost-effective manner.

This requires a need for an alternative solution for the storage of these documents in the decentralized system.

**IPFS** (Interplanetary File System) is a peer-to-peer file storing and sharing system that contains several communications protocols in a decentralized distributed system. It allows to store and share documents in institutions data storage systems and connects them in the global file system [13]. Fig. 3 shows the process flow of IPFS.

Having a content addressable storage, the documents cannot be forged or tampered allowing for an immutable system.

An institution can access and retrieve these documents by calling the hash of the file that is required.

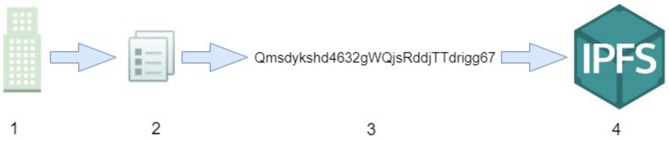


Fig. 3. Interplanetary File System

Steps in IPFS for issuing authority:

1) An issuing authority generates the documents and uploads it in the Interplanetary File System.
2) This institution puts the documents in its data storage systems.
3) The institution adds these documents into the global file system using IPFS which generates a hash value for each document.
4) These documents are then available in the global file system for others to access.

Steps in IPFS for access by institutions:

1) To access the documents provided by the issuing authorities, institutions require the hash values to be shared by those authorities.
2) These institutions can access the copy of the documents through the global file system.
3) The documents can be accessed by using the hash values of each file generated by the IPFS.
4) This allows to locate the file and retrieve a copy of the documents.

The hash value generated by the IPFS is unique to the file and the only way to access the file in the global file system. However, the hash value is not unique to the client accessing the file allowing anyone to access it as long as they have the hash value. This results in poor technique in sharing confidential documents.

The solution for the above problem is achieved using asymmetric encryption. Asymmetric encryption is the use of public and private key to encrypt and decrypt the file. This allows only the specific recipient to access the file as other institutions cannot decrypt it even if they have the hash function.

The file is encrypted with the receiver's public key after which a hash value is generated. This hash value is shared with the recipient who can assess the file through the global file system and decrypt the file using their private key.

The Interplanetary file system can be used along with blockchain to share data over a decentralized system with all the other institutions present in the blockchain as nodes. As documents cannot be stored directly on the blockchain, the files can be stored on the IPFS with their hash values being shared over the blockchain. This provides a secure way to share documents among institutions in fast and cost effective manner.

Fig. 4 shows how files are shared with institutes that need to verify the identity of individuals. It is as follows:

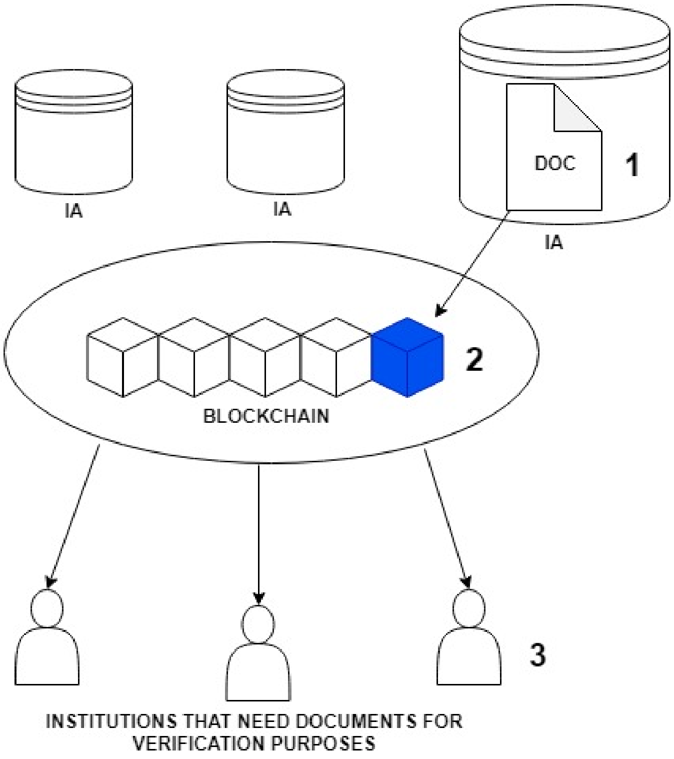


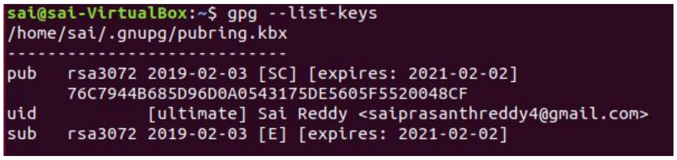
Fig. 4. Process Flow for File Sharing

1) It denotes the Issuing Authorities(IA) data store. Here once the identity document is created it is stored using the IPFS file sharing system.
2) After the file has been stored using IPFS a hash value for that file is created. These hash values are stored onto the blockchain network. Each block gets added with a number of these hash values.
3) Institutions that are a part of the Access client list(ACL) are only able to access the network to get a particular document. Each document has several hash values specific to an institute part of the ACL. The hash key is shared by the individual with these institutes to verify his identity.

### *B. Implementation*

The following implementation of IPFS with asymmetric encryption was done using 2 participants with Linux machines. The participating nodes are installed with GPG for asymmetric encryption and IPFS for storage and sharing of documents. The following steps show the process of encryption and sharing of a document between the two nodes.

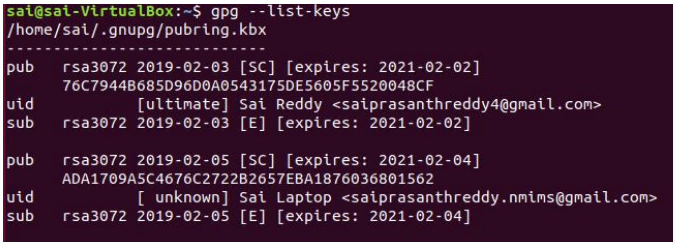
1) Using the command gpg –list-keys in the terminal the list of keys present on that node can be viewed as shown in Fig. 5. This list initially consists of the only one key which belongs to that node.



```
sai@sai-VirtualBox:~$ gpg --list-keys
/home/sai/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2019-02-03 [SC] [expires: 2021-02-02]
      76C7944B685D96D0A0543175DE5605F5520048CF
uid           [ultimate] Sai Reddy <saiprasanthreddy4@gmail.com>
sub   rsa3072 2019-02-03 [E] [expires: 2021-02-02]
```

Fig. 5. Initial List Of Keys

2) After sharing the keys with the other node, both lists contain 2 keys each as shown in Fig. 6. These keys are used to encrypt the document so that only the node whose public key was used to encrypt the file can access it.

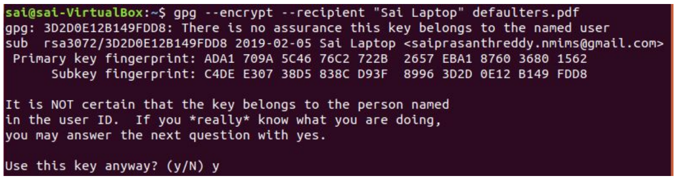


```
sai@sai-VirtualBox:~$ gpg --list-keys
/home/sai/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2019-02-03 [SC] [expires: 2021-02-02]
      76C7944B685D96D0A0543175DE5605F5520048CF
uid           [ultimate] Sai Reddy <saiprasanthreddy4@gmail.com>
sub   rsa3072 2019-02-03 [E] [expires: 2021-02-02]

pub   rsa3072 2019-02-05 [SC] [expires: 2021-02-04]
      ADA1709A5C4676C2722B2657EBA1876036801562
uid           [ unknown] Sai Laptop <saiprasanthreddy.nmims@gmail.com>
sub   rsa3072 2019-02-05 [E] [expires: 2021-02-04]
```

Fig. 6. List Of Keys

3) On the sender node, the encryption of the document is done with the command gpg –encrypt –recipient ”Node name” filename.extention as shown in Fig. 7.



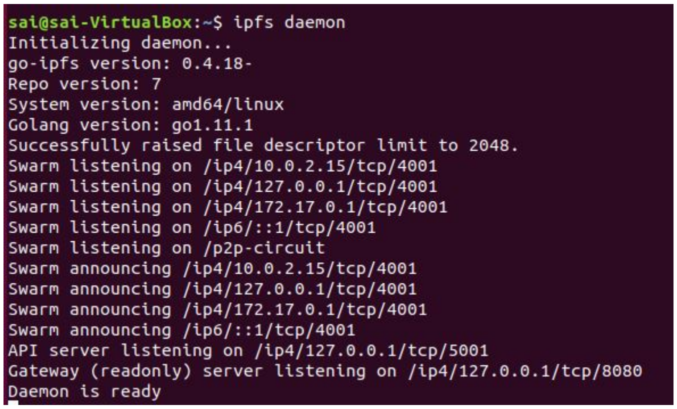
```
sai@sai-VirtualBox:~$ gpg --encrypt --recipient "Sai Laptop" defaulters.pdf
gpg: 3D2D0E12B149FDD8: There is no assurance this key belongs to the named user
sub  rsa3072/3D2D0E12B149FDD8 2019-02-05 Sai Laptop <saiprasanthreddy.nmims@gmail.com>
 Primary key fingerprint: ADA1 709A 5C46 76C2 722B  2657 EBA1 8760 3680 1562
      Subkey fingerprint: C4DE E307 38D5 838C D93F  8996 3D2D 0E12 B149 FDD8

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

Fig. 7. Asymmetric Encryption

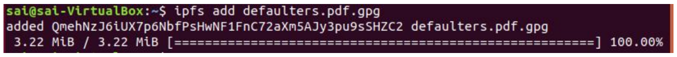
4) To share the document, IPFS is used by running the IPFS daemon with the help of the linux command ipfs daemon as shown in Fig. 8.



```
sai@sai-VirtualBox:~$ ipfs daemon
Initializing daemon...
go-ipfs version: 0.4.18-
Repo version: 7
System version: amd64/linux
Golang version: go1.11.1
Successfully raised file descriptor limit to 2048.
Swarm listening on /ip4/10.0.2.15/tcp/4001
Swarm listening on /ip4/127.0.0.1/tcp/4001
Swarm listening on /ip4/172.17.0.1/tcp/4001
Swarm listening on /ip6/::1/tcp/4001
Swarm listening on /p2p-circuit
Swarm announcing /ip4/10.0.2.15/tcp/4001
Swarm announcing /ip4/127.0.0.1/tcp/4001
Swarm announcing /ip4/172.17.0.1/tcp/4001
Swarm announcing /ip6/::1/tcp/4001
API server listening on /ip4/127.0.0.1/tcp/5001
Gateway (readonly) server listening on /ip4/127.0.0.1/tcp/8080
Daemon is ready
```

Fig. 8. IPFS Daemon

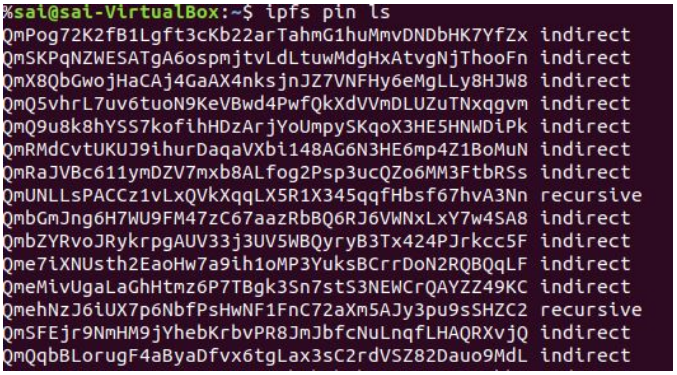
5) Fig. 9 shows the encrypted document being added to the IPFS global file system and the generation of a hash value for that document.



```
sai@sai-VirtualBox:~$ ipfs add defaulters.pdf.gpg
added QmehNzJ6iUX7p6NbfPsHwNF1FnC72aXm5AJy3pu9sSHZC2 defaulters.pdf.gpg
 3.22 MiB / 3.22 MiB [====================================================] 100.00%
```

Fig. 9. Uploading Of Document

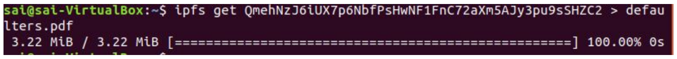
6) On the receiving node, the hash value of the document added to IPFS can be accessed from the list of hash values as shown in Fig. 10.



```
%sai@sai-VirtualBox:~$ ipfs pin ls
QmPog72K2fB1Lgft3cKb22arTahmG1huMmvDNDbHK7YfZx indirect
QmSKPqNZWESATgA6ospmjtvLdLtuwMdgHxAtvgNjThooFn indirect
QmX8QbGwojHaCAj4GaAX4nksjnJZ7VNFHy6eMgLLy8HJW8 indirect
QmQ5vhrL7uv6tuoN9KeVBwd4PwfQkXdVVmDLUZuTNxqgvm indirect
QmQ9u8k8hYSS7kofihHDzArjYoUmpySKqoX3HE5HNWDiPk indirect
QmRMdCvtUKUJ9ihurDaqaVXbi148AG6N3HE6mp4Z1BoMuN indirect
QmRaJVBc611ymDZV7mxb8ALfog2Psp3ucQZo6MM3FtbRSs indirect
QmUNLLsPACCz1vLxQVkXqqLX5R1X345qqfHbsf67hvA3Nn recursive
QmbGmJng6H7WU9FM47zC67aazRbBQ6RJ6VWNxLxY7w4SA8 indirect
QmbZYRvoJRykrpgAUV33j3UV5WBQyryB3Tx424PJrkcc5F indirect
Qme7iXNUsth2EaoHw7a9ih1oMP3YuksBCrrDoN2RQBQqLF indirect
QmeMivUgaLaGhHtmz6P7TBgk3Sn7stS3NEWCrQAYZZ49KC indirect
QmehNzJ6iUX7p6NbfPsHwNF1FnC72aXm5AJy3pu9sSHZC2 recursive
QmSFEjr9NmHM9jYhebKrbvPR8JmJbfcNuLnqfLHAQRXvjQ indirect
QmQqbBLorugF4aByaDfvx6tgLax3sC2rdVSZ82Dauo9MdL indirect
```

Fig. 10. List Of Hash Values

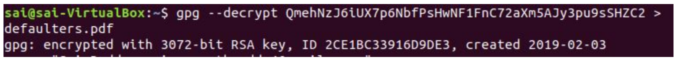
7) The receiving node can then access the document by extracting it from the global file system using it’s hash value. As shown in Fig.11, this downloads a copy of the file on receiver’s machine.



```
sai@sai-VirtualBox:~$ ipfs get QmehNzJ6iUX7p6NbfPsHwNF1FnC72aXm5AJy3pu9sSHZC2 > defau
lters.pdf
 3.22 MiB / 3.22 MiB [==================================================] 100.00% 0s
```

Fig. 11. Downloading The Document

8) The encrypted document needs to be decrypted at the recieving node using it's key as shown in Fig. 12.



```
sai@sai-VirtualBox:~$ gpg --decrypt QmehNzJ6iUX7p6NbfPsHwNF1FnC72aXm5AJy3pu9sSHZC2 >
defaulters.pdf
gpg: encrypted with 3072-bit RSA key, ID 2CE1BC33916D9DE3, created 2019-02-03
```

Fig. 12. Decryption

### C. Discussion

Countries all over the world are moving to blockchain based systems due to their monetary and functional benefits. Dubai is planning on converting to a smart city by 2020 using blockchain technology. It plans on moving all its government operations and some of its banking operations to blockchain based systems to counter check fraud. The projected impacts of this system are immense. Out of the 20 use cases defined, a few have already been implemented. For every 1 billion papers saved by not printing on them, 130 million trees are protected. Hence, overtime, blockchain based systems will continue to prove their monetary and environmental benefits.

From the findings of this implementation, and from the already implemented models of other countries, it is clearly seen that this new system, provides an extremely seamless experience for the users and a highly efficient government. It is technologically advanced as it is reliable, with lesser points of failures. It is reliable as only authentic information can be stored in the blockchain. Security and immutability is also a feature. Since the population of India is drastically more than that of Dubai, it can be predicted that the benefits of this technology in India will be much more.

## Conclusion

Blockchain technology has been coming under the spotlight recently and its utility is universal. The use case of the government described and studied in this paper clearly shows the improvements and benefits of using blockchain based systems over the existing systems. With our findings it is evident that the time taken for document verification is reduced to a fraction compared to current systems taking several weeks. Our model has proven that blockchain based verification is the next evolution for government identity verification process. The environment impact is also highly positive as it is a completely digital process thus saving the need for using paper. A low failure rate in the verification process has also been achieved implying citizens will not need to visit the issuing authorities multiple times. With our model a there is drastic reduction in the number of employees required for the verification process due to its automated nature. This leads to cost benefits in terms of saved paper, saved time and reduced manpower in the institutions. In the future we plan to get the Indian government to implement this model. We also will try to get educational institutes to apply this model for seamless sharing of educational certificates with other institutes for an easier certificate sharing process.

## References

[1] Heng Hou, “The Application of Blockchain Technology in E-government in China”,2017 26th International Conference on Computer Communications and Networks, ICCCN 2017.
[2] Weber I. Gramoli V, Ponomarev A, et.al., “On availability for blockchain-based systems”, Proceedings of the IEEE Symposium on Reliable Distributed Systems (2017).
[3] Ahram T. Sargolzaei A. Sargolzaei S. et.al, “Blockchain Technology Innovations”.
[4] Svein Ølnes and Arild Jansen , ” Blockchain Technology as a Support Infrastructure in e-Government” , DUO 2017.
[5] Vipul H. Navadkar , Ajinkya Nighot , Rahul Wantmure “Overview of Blockchain Technology in Government/Public Sectors” , June 2018 International Research Journal of Engineering and Technology (IRJET).
[6] Ivan Martinovic, Lucas Kello, Ivo Sluganovic , “Blockchains for Governmental Services: Design Principles, Applications, and Case Studies”, December 2017 University of Oxford .
[7] Parol Jalakas, “Blockchain from Public Administration Perspective: Case of Estonia”, Tallinn 2018.
[8] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , ” An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE June 2017.
[9] Harry Halpin and Marta Piekarska , ” Introduction to Security and Privacy on the Blockchain” , IEEE 2017 European symposium.
[10] Using Blockchain and smart contracts for secure data provenance management, Aravind Ramachandran and Dr.Murat Kantarcioglu, September 2017.
[11] Blockgeeks, What is blockchain. Last accessed: March 7, 2019.
[12] Coral Health, Start your own hyperledger blockchain, www.medium.com. Last accessed: March 7, 2019.
[13] Coral Health, Learn to securely share files on blockchain with IPFS, www.medium.com. Last accessed: March 7, 2019.