Reducing Forgery in Land Registry System Using Blockchain Technology

U. M. Ramya(✉), P. Sindhuja, RA Atsaya, B. Bavya Dharani, and SS Manikanta Varshith Golla

Department of Computer Science and Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
um_ramya@cb.amrita.edu, sindhujaparnam@gmail.com, atsyatchul7@gmail.com, bavyabalasubramaniam@gmail.com, satyavrshth6@gmail.com

Abstract. Forgery of land documents is one of the major problems faced by any state government in land registration system. Even though the documents are now secured in the database, but these records can be tampered because there is no proper security and time-stamping present in the database system. To overcome this problem, the use case can be deployed using Blockchain. Blockchain being a distributed system, data is available to everyone in the network. Every block added into the blockchain is time stamped and proof-of-work is required to add the block, making the data very hard to be tampered. In this paper, we have used a private-permissioned Blockchain - Multichain, where the authority lies with the registrar making the process faster because proof-of-work [13] is not required. The implementation of land registration use-case involves recording the documents into blockchain and verifying it with the one stored in digital locker thereby reducing forgery of documents.

Keywords: Multichain · Distributed ledger · Streams · Hash value Consensus protocol · Digilocker

1 Introduction

Blockchain can be understood easily by taking the Bitcoin [1] use case. Smart contracts [3, 5] can be deployed. They are used in various use cases [4] like health care, legal, education, supply chain [2, 7]. Blockchain is a universal digital ledger for recording all transactions or digital events executed by participating parties. Block chain's core technology uses cryptography as well as distributed database architecture that is open ledger and a peer-to-peer protocol to create shared ledgers among different parties. Each transaction before getting added into blockchain is verified using any one of the consensus protocols [9] by the nodes present within the network. Once a block is written into the blockchain, the information in the blockchain is immutable –meaning it cannot be manipulated or erased. The distributed ledger chronologically stores information in "blocks" containing a verifiable record of every single transaction, as well as the sequence in which the transactions were executed. A third party is not required to

A. K. Luhach et al. (Eds.): ICAICR 2018, CCIS 955, pp. 725–734, 2019.
https://doi.org/10.1007/978-981-13-3140-4_65

monitor, manage and validate transactions. Transactions such as money transfers or stock purchases require a third party to monitor and record these activities. In a blockchain, in order to perform any transaction accepted by the rest of the network before adding block into the blockchain, a participant(miner) must show "proof of work" – a mechanism for protecting the integrity of information and preventing fraud. Once captured, information in the blockchain is immutable – meaning it cannot be manipulated or erased.

2 Literature Survey

Presently the records are stored in database. Database is authorised wholly by a single entity, this may lead to single point failure. There is no time stamping in database. ChromaWay [8] a Bitcoin blockchain company is working on land registration using the blockchain technology.

Blockchain Characteristics

- Decentralized data(an open ledger to every node in the network).
- Mutual consensus by participants.
- Use of cryptography.
- Digital signature for identity verification.
- Strict controls and time-stamped data.
- Direct, secure and immediate access to data (which is immutable).

Types of Blockchain

- Public blockchain/Permissionless blockchain [12]
  As the name suggests it is a blockchain of public where there is no in charge to write into the blockchain. But while deploying the land registration use case the government should have the authority so here we use private/permissioned blockchain.
- Private blockchain/Permissioned blockchain [12]
  Permissioned Blockchain type [6] requires permission to connect, read the data on the blockchain, limits the number of participants who can connect, transact on the blockchain and serve the network by creating new blocks into the chain. Eg Ripple [10], Multichain, HyperLedger, Ethereum [11], Hydrachain [14].

Similarities Between Public and Private Blockchain

Both of these are peer-to-peer and decentralised networks avoiding single point failure, where every node in the network has a copy of a shared append-only ledger of digitally signed transactions.

- Both maintain the copies which are consistent through a consensus protocol.
- Both the Blockchains make sure that the data which is present in the blockchain cannot be manipulated even in the presence of completely faulty or malicious node in the network.

Difference Between Public and Private Blockchain

- Nodes participating in the network.
- Nodes executing the consensus protocol.
  A public blockchain network is open and anyone can join the network, can access and read or write data from the ledger. Presently Bitcoin [1] is one of the largest public blockchain networks. The major drawback of a public blockchain is very high consumption of computational power required by the miners to solve complex problems and produce proof-of-work. When a new node wants to join the private blockchain network, it requires permission to connect to the network which is given by the blockchain creator. Organisations that deploy a private blockchain will generally use a permissioned network. So there are restrictions on who can be part of the network, and only in particular transactions. The privileges given to the nodes in the network differ. In order to join the network, nodes need to get permission from the network creator. Nodes existing in the network depending on their privilege get to decide new joiners into the network. A regulatory authority or consortium could issue licenses for participation. Once a node enters the network, it maintains the blockchain in a decentralized manner. The creator of the blockchain has the authority to make the records available for every node present in the network to read, but the privilege to write/add the blocks is not given to every one in the network keeping in mind the security of the network and mining. With permissioned Blockchains, it's not mandatory to use POW (Proof-of-Work) for achieving consensus from the nodes which actually requires high computational power or some other system requirement.

3 System Architecture

Figure 1 given below shows the overall view of our proposed system. The proposed system is explained in the following steps

1. If the seller wants to sell the land he should have the hard copy of the land document and soft copy of the same i.e. present in the digilocker [15] (which gets uploaded by the government).
2. The sender will send the copy to the registrar.
3. The registrar converts the received soft copy of the document into hash value and verifies the hash value of the corresponding document i.e. already present in the blockchain.
4. At the same time the buyer witnesses the whole process. If he is convinced with the process he will registrar to transfer the ownership from the seller to buyer.
5. The registrar prepares the hard copy of the new document.
6. The registrar scans the document and puts it into the database of the government.
7. When the buyer requests the government for the document he should be able to get the soft copy of the document into his digilocker account.
8. The registrar should convert the scanned document into a hash value and upload it into the blockchain.

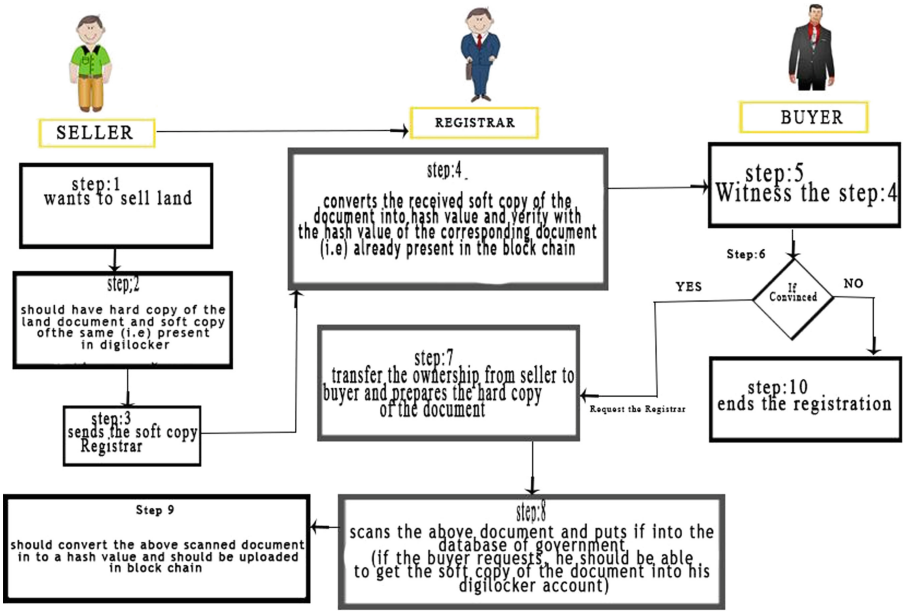

Fig. 1. System architecture

4 Implementation

In this proposed system, we have used Multichain platform to deploy the land registration use case. It is a readily available platform for the creation and deployment of private Blockchains, either within or between the organizations. It provides the privacy and control required in a easy-to-use package. Multichain supports Windows, Linux and Mac servers and provides a simple API and command-line interface. Multichain solves the problems of mining, privacy and openness through coordinated management of user permissions. The main functionality 'Streams' implemented in Multichain platform enable blockchain to be used as an all-purpose append-only database, with the blockchain providing time stamping, notarization and immutability of documents present in it. There is no constraint on the number of streams that could be created. The restriction is, items can only be added to it. Each item that gets added to the stream represents a blockchain transaction. Without knowing the underlying mechanism, developer scan read and write streams. The vital part of streams is in indexing and retrieval. Each participant in the network can subscribe to any stream of their choice with the blockchain making sure of consistency of the open ledger. As Blockchain is a peer-to peer decentralized network, items in a stream gets added from various nodes across the network irrespective of the order of arrival.

Multichain-Console Commands

The Following are the steps to be followed in a console for creating and dealing with Multichain private blockchain:

1. Creating a Blockchain
server1:
multichain-util create chain1
2. To Initialize
server1:
multichain-util create chain1
On doing so, IP address and port number is obtained.
3. Connecting the Blockchain
Server2:
multichaind chain1@[ip-address]:[port]
Server2 is added to the list of peers.
4. To Get Permission
Server1: multichain-cli chain1 grant 1.
connect, receive
5. To Switch to Interactive Mode
On both servers:
multichaind chain1 –daemon
6. Creating a Stream
Server1:
create stream stream1 false
7. To Publish into Stream
Server1:
publish stream1 key1 73747265616d2064617461
8. To Subscribe to this Stream and View its Contents
Server2:
1. liststreams
2. subscribe stream1
3. liststreamitems stream1

5 Limitations

Since blockchain technology is a new technology, it is still in an emerging state across industries. The real implementation of the system is very costly, and hence system is developed in a testing environment. Computational power is a major limitation for a public blockchain which can be overcome by private one. Since even a small change to the original hard copy of the document (e.g.: ink mark, letters getting faded, etc.) will affect the hash value drastically, a digital copy of the document should be present with the owner. digilocker app can be used to have the permanent soft copy of the document since it can't be deleted.

6 Sample Screen Shots of Implementation of Land Registration Use-Case

See Figs. 2, 3, 4, 5, 6, 7 and 8.

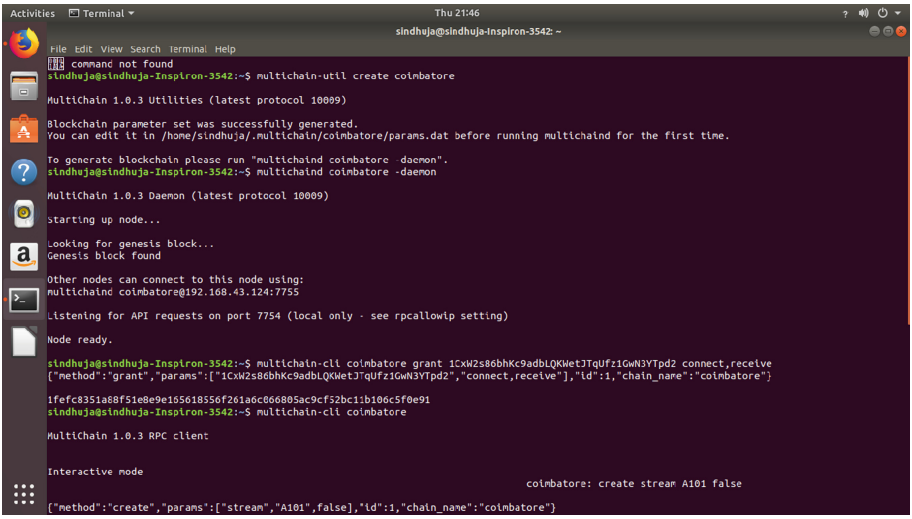

Fig. 2. Creation of the Blockchain "Coimbatore" from the Host server (registrar)

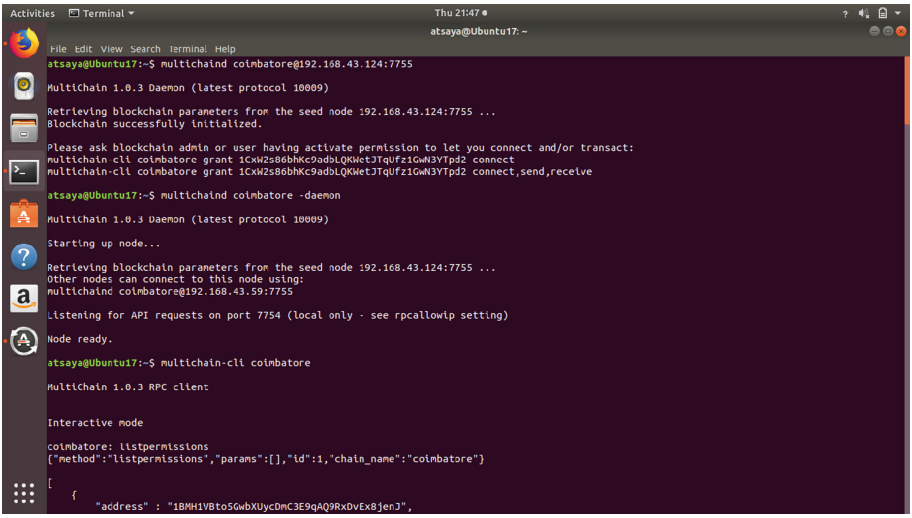

Fig. 3. Connecting to the created Blockchain by the buyer from his server.

7 Future Work

The proposed work can be extended and implemented in practical use. Since there are chances for the document to get spoilt atleast a little after several years, digital copy of the document must be present and carried with the original document to proceed with transaction. Because even a very small change such as an ink mark on the paper will generate a drastically different hash and hence the authentication will be difficult to be

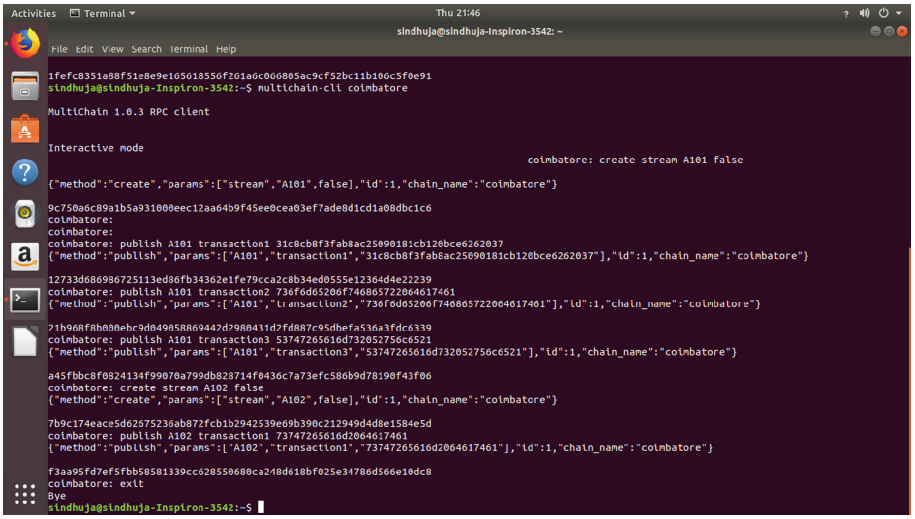

Fig. 4. Creating stream "A101" and putting the hashed documents into the Blockchain

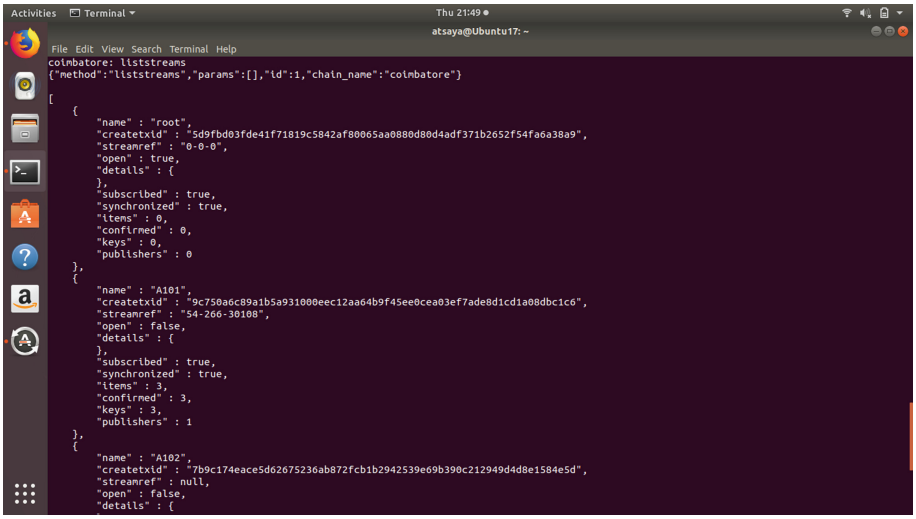

Fig. 5. To find the available land streams in the Blockchain by the buyer

verified. Thus to make it simple, the soft copy of the document must be updated in the government database so that any time when the owner asks for the copy it can be given. And also the government can take initiative to make the land documents available to the owner through the digilocker app. As mentioned earlier, once data is put in the digital locker it cannot be deleted by the user. This prevents us from losing the softcopy of the document.

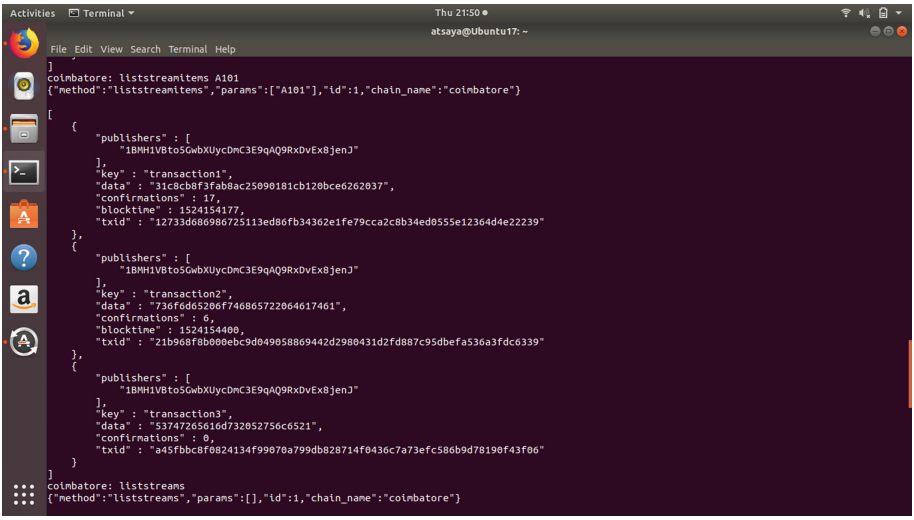

Fig. 6. To see the transactions for the land “A101” by the buyer

hex: 31c38cb8f3fabf8ac25090181c6120bce6262037

HEX: 31C38CB8F3FABF8AC25090181C6120BCE6262037

h:e:x: 31:c3:8c:b8:f3:fa:bf:8a:c2:50:90:18:1c:61:20:bc:e6:26:20:37

base64: McOMuPP6v4rCUJAYHGEgvOYmlDc=

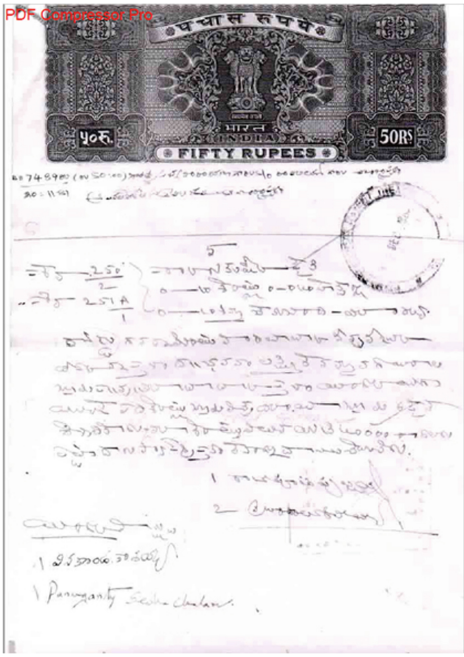

Fig. 7. Hash value of original document

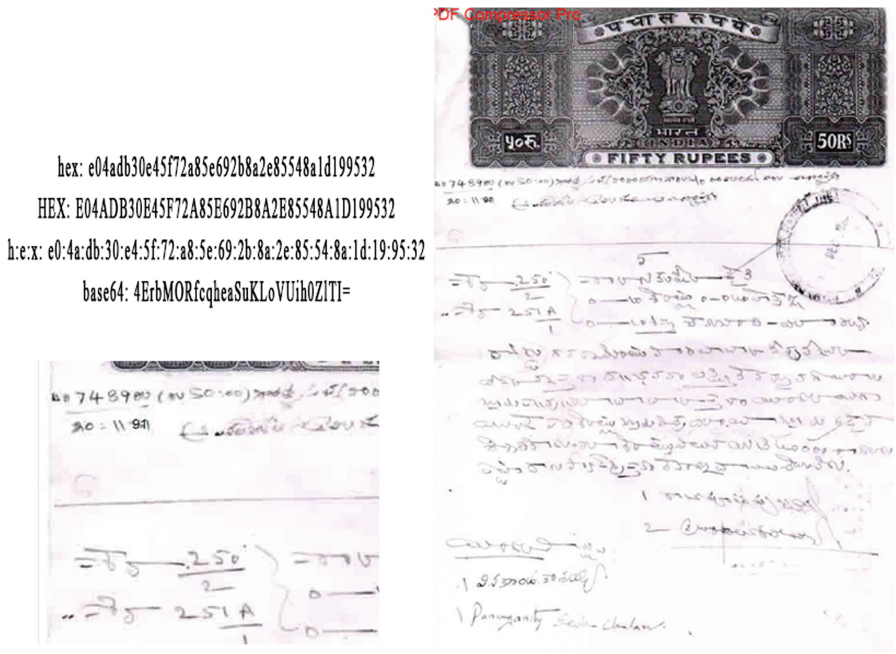

Fig. 8. Hash value after a change in doucment

8 Conclusion

Thus, the use-case land forgery prevention is achieved with the blockchain technology. Unlike current existing system, the document as such cannot be viewed by the buyer since the hashed value of the document only is available (because a hashed value cannot be de-hashed) thus providing user's privacy. The documents cannot be claimed by someone later by tampering because it changes the hash value and hence the transaction will become invalid and will not be proceeded further. Another advantage is that the time-stamp of the original document created in the blockchain will be used to cross-verify and thus the document and the land becoming totally safe. This system thus helps in a complete forgery less land transaction.

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. White Paper (2008)
2. The Blockchain Imperative: The Next Challenge for P&C Carriers. Cognizant
3. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the Blockchain model of cryptography and privacy- preserving smart contracts. In: 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, pp. 839–858 (2016). https://doi.org/10.1109/sp.2016.55

4. Implementing Blockchain for cognitive IOT applications: integrate device data with smart contracts in IBM Blockchain. IBM Developer Works
5. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
6. Nugent, T., Upton, D., Cimpoesu, M.: Improving data transparency in clinical trials using blockchain. Firstpublished: 20 Oct 2016, 2541 Latest published 20 Oct 2016, 2541
7. Archa, A.B., Achuthan, K.: Trace and track: enhanced pharma supply chain infrastructure to prevent fraud. In: Kumar, N., Thakre, A. (eds.) Ubiquitous Communications and Network Computing. UBICNET 2017. Lecture Notesof the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 218. Springer, Cham (2018)
8. Mizrahi, A.: A blockchain-based property ownership recording system
9. Siva Sankar, L., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on Blockchain applications. In: 2017 International Conference on Advanced Computing and Communication Systems (ICACCS 2017), Jan. 06–07 (2017). Coimbatore, INDIA
10. Schwartz, D., Youngs, N., Britto, A.: The ripple protocol consensus algorithm (2014)
11. Multichain. https://www.multichain.com/
12. On Public and Private Blockchain. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains
13. Blockchain: What is in a block? https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo
14. Hydrachain. https://github.com/HydraChain/hydrachain
15. https://www.ndtv.com/business/list-of-documents-you-can-store-on-digilocker-from-aadhaar-card-to-your-pan-card