http://dx.doi.org/10.21172/ijiet.181.05

# Recording Unique Digital Identity on Blockchain Platform

Tripti Rathee[1]
*[1]Assistant Professor*
*Maharaja Surajmal Institute of Technology*
*C-4, Janakpuri*
*New Delhi*

**Abstract - The paper focuses on the use of blockchain and distributed ledger technology for government services and digital identity in relation to those. The essential features are that a blockchain has no central data controller or storage and that it is an append-only immutable record, store with reliable timestamping, thus can be used to help the refugee identity crisis by authenticating and storing their digital id on blockchain platform. Worldwide, the refugees face a general identity problem in which the paper-based identity systems cannot be used across borders here because the government which would usually serve as a guarantor may be hostile, unreachable or may not exist as a functioning entity. They need a secure platform to store and authenticate their identities with a unique hash and timestamp which can be further used by the host country or organisations like UN.**

**Keywords: Blockchains, Digital Identity, Storing data.**

## I. INTRODUCTION

The issue of garnering trust is of utmost importance in communicating systems especially when they are dealing with sensitive data. IoT visualizes a fully connected world where each and every smart device is connected to each other and they collaborate to perform specific tasks. Trust is the main essence especially when there is no audit mechanism in place, so it needs to be taken care of [1]. Ever since Satoshi Nakamoto in his paper [2] described the Blockchains, the people all over the globe are devising ingenious ways in which the concept can be applied to solve certain issues related to various fields. Blockchain has the potential to change the way that the world approaches data. Basically, blockchain is a peer-to-peer network where the interconnected systems are fully open and transparent to each other [3]. The data is stored in a block, and each block contains previous hash as well as the hash to the next block. Each member node of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction [4]. To support blockchains and operate with the blockchain, network peers have to provide, the following functionality: routing, storage, wallet services and mining [5].

The Routing function is necessary to participate in the P2P network; this includes transaction and block propagation. The storage function is responsible for keeping a copy of the chain in the node (the entire chain for full nodes, and only a part of it for light nodes). Wallet services provide security keys that allow users to order transactions, i.e., to operate with their Bitcoins. Finally the mining function is responsible for creating new blocks by solving the proof of work [5] .The system is an incorruptible, distributed, transparent, immutable, secure and auditable digital ledger having distributed digital information chronologically arranged in a transaction table, maintained by multiple entities [6].

Private Blockchains are used in this research paper, an authority holds the sole right for authorizing write/read permissions and mine blocks. Only the authorized nodes can access block requests and access the data. Private Blockchains finds it application as extremely secure database for banking and other related sector where data security is utmost priority since it is managed by a trusted party and the encrypted database is commonly shared. Bankchain, Multichain, Blockstack are some of the examples of Private Blockchain [7]. The basic structure of mining has been presented in figure 1.

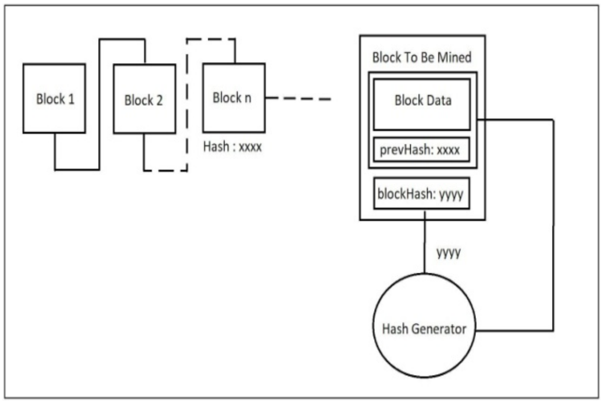


Fig. 1: Block mining to the transaction table

The emergence of blockchain technology offers significant opportunities for the provision of decentralized services in a trustless or low trust setting, with decentralization, in particular, being relevant for cross-border applications. Blockchain serves as a bookkeeping platform or ledger that is incorruptible, enforces transparency, and bypasses censorship [1][4].

By tackling issues of financial, political and institutional corruption, this has the potential to create massive social change and greatly protect the human rights of every individual. Digital identity is effectively the core use case for blockchains for government services, spanning all others discussed here. Providing or interpreting proof that individuals are who they claim to be, and are the subjects of government records, are the prerequisites for the provision of services, recognition of rights or title, or of duties required or fulfilled.

In this paper the purpose of using the Blockchain is to have a transparency of data so that the authorities can have a very clear knowledge of recording unique digital identity. The study focuses on getting the data in the form of registrations and then the data can be used by the governments(s) so that they can prevent the illegal migrations. It is no great surprise, then, that identity has received a great deal of attention from governments globally as an application of blockchain. Identity is an important question for many scenarios, public or private, but more so for the context of interactions with a state; property, health, voting, finance and taxation, education, and so on, all have significant relevance for an individual's life, and there are major, often legal, implications for interactions between individuals and government in these areas.

## II. LITERATURE SURVEY

The emergence of blockchain technology was introduced in [1]. The authors in [1] have proposed a peer-to-peer network using proof-of-work to record a public history of transactions. Ethereum is one of A next generation smart contract and Decentralized application platform which works on blockchain technology [2].The authors in[3] have described a protocol called NFB (it stands for Notarizing Files over the Blockchain). This protocol ensures the communication between two systems: a permissive Blockchain and a secured centralized Document Management System. This paper [4] describes industry use cases that drive the principles behind a new blockchain fabric, and outlines the basic requirements and high level architecture based on those use cases. The authors in [5] have claimed that Blockchain recordkeeping could increase transparency, protect privacy, improve efficiency, and even help guard against obsolescence. Recordkeeping risks must be investigated and mitigated. Quorum is ideal for any application requiring high speed and high throughput processing of private transactions within a permissioned group of known participants [6].The authors in [7] have referred to the Blockchain technology that will lead to innovation and transformation of governmental processes. They have presented a critical assessment of the often exaggerated benefits of blockchain technology found in the literature and discuss their implications for governmental organizations and processes. The authors in [8] have argued that we need to look beyond the currency applications and investigate the potential use of the blockchain technology in governmental tasks such as digital ID management and secure document handling. The authors in [9] suggests that Blockchain technology, widely acknowledged as enabling openness, can facilitate the development of an immutable, transparent, secure and verifiable application for capturing individuals Intellectual Property as they work. The authors in [10] have proposed a query notary for biomedical data consumers (humans or programs alike) who need to retrieve accurate and certified data from reference biomedical databases. The authors in [11] have presented peer-reviewed papers bringing together academia and industry to analyze problems ranging from deploying newer cryptographic primitives on Bitcoin to enabling use-cases like privacy-preserving file storage. The authors in [12] have provided proofs on appropriate and novel assumptions on the “hashing power” of the adversary relative to network synchronicity. The authors in [13] have suggested a protocol that turns a block chain into an automated access-control manager that does not require trust in a third party. The authors in [14] have provided a literature survey on blockchain security issues and challenges. The authors in [15] have provided rationales to support the architectural decision on whether to employ a decentralized blockchain as opposed to other software solutions, like traditional shared data storage. The authors in [16] have demonstrated a blockchain-based solution for transparently managing and analyzing data in a pay-as-you-go car insurance application. The authors in [17] have demonstrated that the scientific credibility of findings from clinical trials can be undermined by a range of problems including missing data, endpoint switching, data dredging, and selective publication. The authors in [18] claim that by combining the decentralized blockchain principle with identity verification, a digital ID can be created that would act as a digital watermark which can be assigned to every online transaction.

## III. RESEARCH METHODOLOGY

Depending upon authorization of adding an entry into the blocks into blockchain, the blockchains can majorly be classified into public, private and permission less/consortium blockchains [7].In Public Blockchain, any individual may access the information, do the transactions and participate in the consensus procedures therein[20]. An authority exists which sanctions mining rights and authorized nodes can take decision to append or not to append in the blockchain. In Private Blockchains, an authority holds the sole right for authorizing write/read permissions and mine blocks[21]. Only the authorized nodes can access block requests and access the data. In Permission less/Consortium blockchains, no single entity in blockchain network is authorized with ability to grant or revoke permission and neither any entity or node is entitled with authority to add items to blockchain.

Worldwide, the refugees face a general identity problem in which the paper-based identity systems cannot be used across borders because the government which would usually serve as a guarantor may be hostile, unreachable or may not exist as a functioning entity. They need a secure platform to store and authenticate their identities with a unique hash and timestamp which can be further used by the host country or organisations like UN. The main objective of our project is that even in less traumatic cases of the international movement, the reliance on an individual’s home government could be lessened by a secure digital identity service based on the blockchain, reducing the number of parties involved in interaction and potentially increasing efficacy and trust by putting the data over Blockchains. Basically, blockchain is a peer-to-peer network where the interconnected systems are fully open and transparent to each other [3]. The data is stored in a block, and each block contains previous hash as well as the hash to the next block. Each member node of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction.[4] To support blockchains and operate with the blockchain, network peers have to provide, the following functionality: routing, storage, wallet services and mining [5]. The Routing function is necessary to participate in the P2P network, this includes transaction and block propagation. The storage function is responsible for keeping a copy of the chain in the node (the entire chain for full nodes, and only a part of it for light nodes). Wallet services provide security keys that allow users to order transactions, i.e., to operate with their Bitcoins. Finally the mining function is responsible for creating new blocks by solving the proof of work [5]. The system is an incorruptible, distributed, transparent, immutable, secure and auditable digital ledger having distributed digital information chronologically arranged in a transaction table, maintained by multiple entities [6]. The main objective of our project is to limit the usage of paper based identification methods and promote and encourage the more techno-friendly platform to store and authenticate the identities with a unique hash and timestamp, which is known as blockchain [19]. We have done coding for blockchain in JavaScript and The Database is implemented using LevelDB (Google).The flow graph has been represented in figure 2.

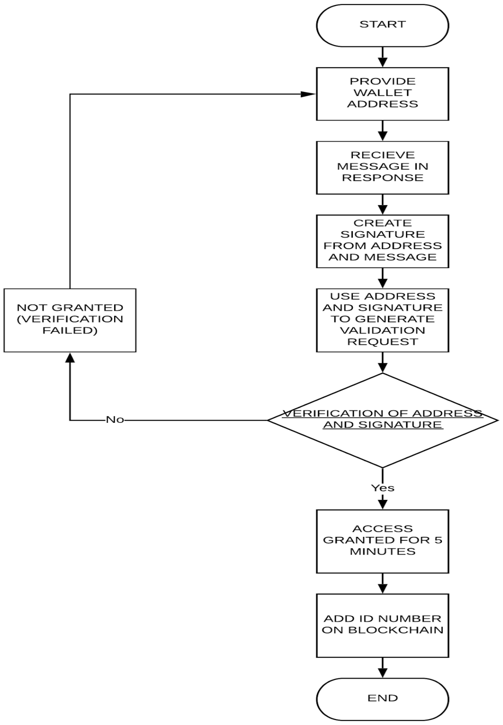

START
PROVIDE WALLET ADDRESS
RECIEVE MESSAGE IN RESPONSE
CREATE SIGNATURE FROM ADDRESS AND MESSAGE
USE ADDRESS AND SIGNATURE TO GENERATE VALIDATION REQUEST
NOT GRANTED (VERIFICATION FAILED)
No
VERIFICATION OF ADDRESS AND SIGNATURE
Yes
ACCESS GRANTED FOR 5 MINUTES
ADD ID NUMBER ON BLOCKCHAIN
END

Fig.2: Process Flowchart

The main objective of our research is to help the refugee identity crisis by authenticating, storing their digital id and putting the data over Blockchains so that any case of unauthorized identity manipulation can be immediately reported to the concerned government agencies. We have done coding for blockchain in JavaScript and The Database is implemented using LevelDB (Google). For achieving this we have adopted the following methodology:

1) The API is used to make the first request in terms of validating the wallet address. Each validation of the wallet address can be used just once to register a Digital Identity, and must be validated again to register a second one. An address is like a single-use token. You can send bitcoins to a person by sending bitcoins to one of their addresses. However, unlike e-mail addresses, people have many different Bitcoin addresses and a unique address should be used for each transaction[13].

2) To validate the wallet address sent in the first request, we need to create a signature from the message returned in the API.

3) The access will be granted for 5 mins or for just one registration and within that time the data/ ID number of the refugee, person will be added to it the Blockchain.

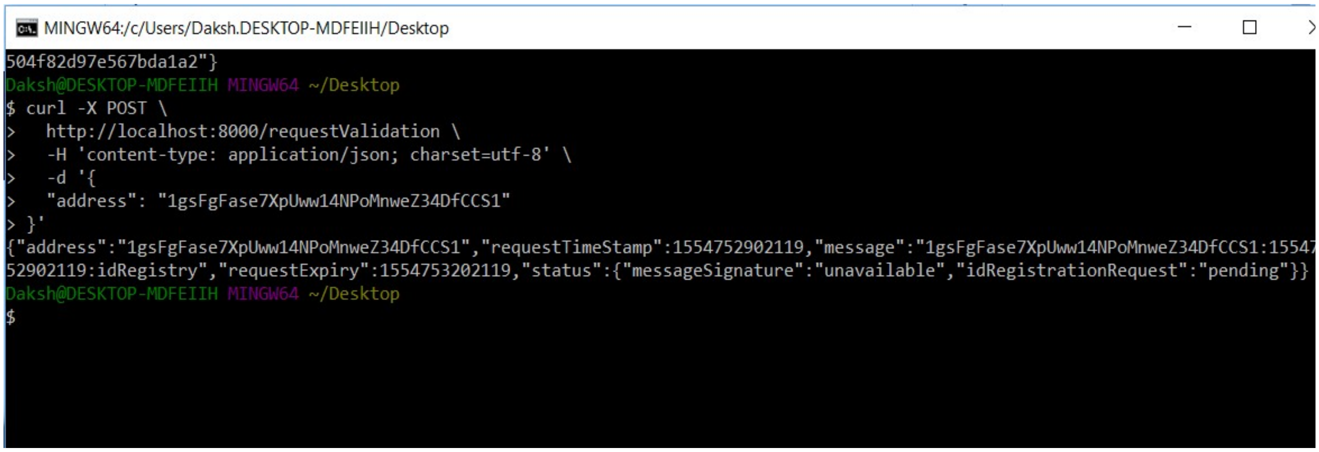
4) All the concerned government agencies can see all the digital identities to a specific wallet address by providing address as a parameter. If there is any change in the identity number of the person the block hash would change, while the chain is validating it would return an error on terminal and administrator would be notified immediately.

## IV. RESULTS

We have created a private blockchain using Javascript, its various frameworks and libraries like NPM (Node Package Manager) which is responsible for managing all our NodeJS packages and modules, Crypto-js JavaScript Library used for crypto standards, Express.js A flexible Node.js web application framework that provides a robust set of features for web and mobile applications, Level A Node.js wrapper for abstract-leveldown compliant stores, which follow the characteristics of LevelDB, bitcoinjs-lib a Bitcoin library for NodeJS etc.

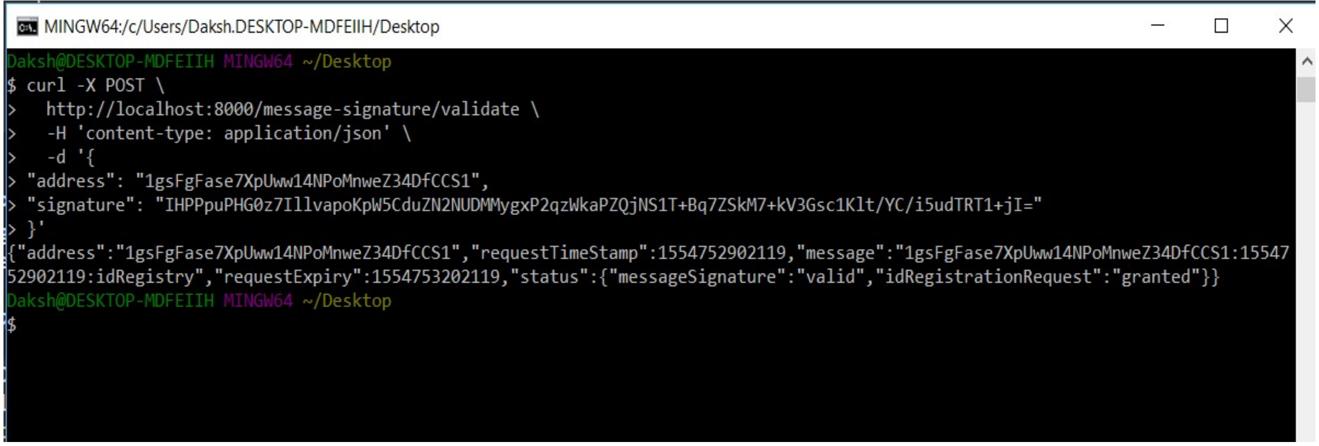
The Database Storage is administered by LevelDB. It is a simple key-value pair database built by Google. The User is asked to validate the wallet address, each validation of the address can be used just once, and must be validated again to for each request. To validate the wallet address sent in the first request, the user needs to create a signature from the message returned in the API, then send the signature and the wallet address to the API to validate the wallet signature. The User then can add data to the Blockchain once within the next 5 minutes of validation, after that the user has to send a request for validation again. This is a security feature that prevents a user from misusing it by sending multiple requests at a time.

The following screenshots represent various stages during the implementation of the Private Blockchain as mentioned above.



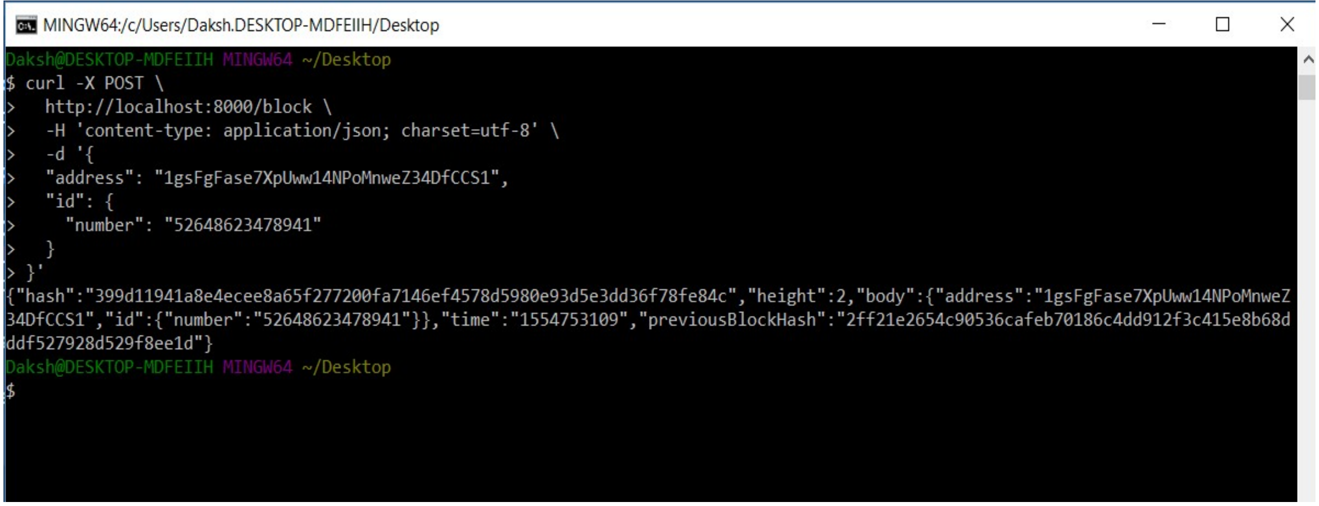
```
504f82d97e567bda1a2"}
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$ curl -X POST \
>   http://localhost:8000/requestValidation \
>   -H 'content-type: application/json; charset=utf-8' \
>   -d '{
>   "address": "1gsFgFase7XpUww14NPoMnweZ34DfCCS1"
> }'
{"address":"1gsFgFase7XpUww14NPoMnweZ34DfCCS1","requestTimeStamp":1554752902119,"message":"1gsFgFase7XpUww14NPoMnweZ34DfCCS1:15547
52902119:idRegistry","requestExpiry":1554753202119,"status":{"messageSignature":"unavailable","idRegistrationRequest":"pending"}}
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$
```

WrittenFig.3: Post request and response for requesting validation



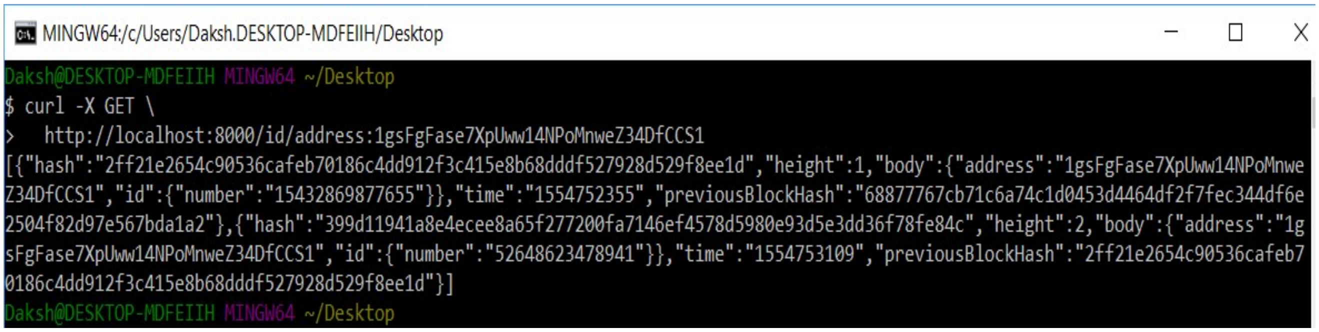
```
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$ curl -X POST \
>   http://localhost:8000/message-signature/validate \
>   -H 'content-type: application/json' \
>   -d '{
> "address": "1gsFgFase7XpUww14NPoMnweZ34DfCCS1",
> "signature": "IHPPpuPHG0z7IllvapoKpW5CduZN2NUDMMygxP2qzWkaPZQjNS1T+Bq7ZSkM7+kV3Gsc1Klt/YC/i5udTRT1+jI="
> }'
{"address":"1gsFgFase7XpUww14NPoMnweZ34DfCCS1","requestTimeStamp":1554752902119,"message":"1gsFgFase7XpUww14NPoMnweZ34DfCCS1:15547
52902119:idRegistry","requestExpiry":1554753202119,"status":{"messageSignature":"valid","idRegistrationRequest":"granted"}}
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$
```

Fig.4: POST request for message signature verification



```
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$ curl -X POST \
>   http://localhost:8000/block \
>   -H 'content-type: application/json; charset=utf-8' \
>   -d '{
>   "address": "1gsFgFase7XpUww14NPoMnweZ34DfCCS1",
>   "id": {
>     "number": "52648623478941"
>   }
> }'
{"hash":"399d11941a8e4ecee8a65f277200fa7146ef4578d5980e93d5e3dd36f78fe84c","height":2,"body":{"address":"1gsFgFase7XpUww14NPoMnweZ
34DfCCS1","id":{"number":"52648623478941"}},"time":"1554753109","previousBlockHash":"2ff21e2654c90536cafeb70186c4dd912f3c415e8b68d
ddf527928d529f8ee1d"}
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$
```

Fig.5: POST request to add a block on the chain with ID number as body parameter.



```
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
$ curl -X GET \
>   http://localhost:8000/id/address:1gsFgFase7XpUww14NPoMnweZ34DfCCS1
[{"hash":"2ff21e2654c90536cafeb70186c4dd912f3c415e8b68dddf527928d529f8ee1d","height":1,"body":{"address":"1gsFgFase7XpUww14NPoMnwe
Z34DfCCS1","id":{"number":"15432869877655"}},"time":"1554752355","previousBlockHash":"68877767cb71c6a74c1d0453d4464df2f7fec344df6e
2504f82d97e567bda1a2"},{"hash":"399d11941a8e4ecee8a65f277200fa7146ef4578d5980e93d5e3dd36f78fe84c","height":2,"body":{"address":"1g
sFgFase7XpUww14NPoMnweZ34DfCCS1","id":{"number":"52648623478941"}},"time":"1554753109","previousBlockHash":"2ff21e2654c90536cafeb7
0186c4dd912f3c415e8b68dddf527928d529f8ee1d"}]
Daksh@DESKTOP-MDFEIIH MINGW64 ~/Desktop
```

Fig 6: Blocks/IDs registered to a specific address

## V. CONCLUSION AND FUTURE SCOPE

The work will give transparency and authenticity of the identity data of refugees seeking asylum in the western countries. The free movement of people across the EU(the hub of refugee crisis) brings with it the need for citizens to interact with and use government services outside their countries of origin, in many or all of the contexts in which those services are accessed by citizens of the host country. Asset registries, currency, healthcare, voting, taxation and education are not only needed within a country but also, more specifically, between countries, to account for the (common) situation in which an individual need to access services across borders. In future, we will try to integrate third party applications like Digilocker with this blockchain platform to verify/add data of different IDs and to implement mobile app viewing of the digital identity documents.

## REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[2] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*, 1-32.
*[3]* Magrahi, H., Omrane, N., Senot, O., & Jaziri, R. (2018, February). NFB: A Protocol for Notarizing Files over the Blockchain. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security*
[4] Dhillon, V., Metcalf, D., & Hooper, M. (2017). The hyperledger project. In *Blockchain enabled applications* (pp. 139-149). Apress, Berkeley, CA.
[5] Lemieux, V. L. (2017). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems. In *Future Technologies Conference (FTC)* (Vol. 2017).
[6] Morgan, J. P. (2016). Quorum whitepaper. *New York: JP Morgan Chase*.
[7] Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.
[8] Ølnes, S., & Jansen, A. (2017, September). Blockchain technology as s support infrastructure in e-government. In *International Conference on Electronic Government* (pp. 215-227). Springer, Cham.
[9] O'Leary, K., O'Reilly, P., Feller, J., Gleasure, R., Li, S., & Cristoforo, J. (2017, August). Exploring the application of blockchain technology to combat the effects of social loafing in cross functional group projects. In *Proceedings of the 13th International Symposium on Open Collaboration* (p. 13). ACM.
[10] Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2018). Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In Precision Medicine Powered by pHealth and Connected Health (pp. 69-73). Springer, Singapore.
[11] Halpin, H., & Piekarska, M. (2017, April). Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-3). IEEE.
[12] Garay, J., Kiayias, A., & Leonardos, N. (2015, April). The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 281-310). Springer, Berlin, Heidelberg.
[13] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180-184). IEEE.
[14] Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, *19*(5), 653-659.
[15] Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016, April). The blockchain as a software connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182-191). IEEE.
[16] Vo, H. T., Mehedy, L., Mohania, M., & Abebe, E. (2017, November). Blockchain-based data management and analytics for micro-insurance applications. In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management* (pp. 2539-2542). ACM.
[17] Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, *5*.
[18] Jacobovitz, O. (2016). Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva*.
[19] Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. *arXiv preprint arXiv:1806.03693*.
[20] Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.".
[21] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE.