Matrimony Website using Blockchain for Tracking Authenticity of Profiles

Prof. Smita Pai[1], Rachana Parkar[2], Megha Gajare[3], Onkar Patil[4]

[1]*Assistant Professor, Dept. of Information Technology, Terna Engineering College, Nerul, Navi Mumbai, India*
[2]*Student, Dept. of Information Technology, Terna Engineering College, Nerul, Navi Mumbai, India*
[3]*Student, Dept. of Information Technology, Terna Engineering College, Nerul, Navi Mumbai, India*
[4] *Student, Dept. of Information Technology, Terna Engineering College, Nerul, Navi Mumbai, India*

***

Abstract – *Blockchain is a transparent and secure network. It is rapidly getting attention from companies who wish to change from centralized to decentralized system. This paper proposes a system for matrimony website using blockchain for tracking authenticity of profiles. A prototype demonstrates the application of blockchain in identity and access management using the truffle development network. Basic Authentication operations such as saving the user activity log are able to execute in negligible time.*

Key Words: Identity management, Matrimony, Blockchain, Ethereum, Decentralization, Web3 Js, Metamask, Solidity.

1. INTRODUCTION

Decentralized networked platforms are getting increasing attention due their features such as Trust and Transparency, Data security and privacy, Scam and fraud free activities. The cryptocurrencies such as Bitcoin and Ether uses decentralized network [1]. Blockchain can be defined as the chain of blocks or ledgers of information which are linked to each other with cryptography. The blockchain does not require a centralized trusted authority since it is distributed all over the participants nodes. Whenever a block is getting added in the chain, majority of the nodes in the network must validate the block to eliminate the problem of malicious information altering of the block [1]. This ensures the integrity of the blockchain given that the majority of the nodes can be trusted.

Identities of resources in a system can be obtained by using public key cryptography. In public key cryptography, such as RSA, the public-private key pair is unique for the issuing entity and only the one who owns a matching private key can sign a message, whereas everyone else can validate the authenticity of the message by using the public key [1]. Without the involvement of central authority (CA), identity can be created by generating a new public-private key pair.

This paper explores the potential of identity management in blockchain technology applied to a decentralized matrimonial web application. It discovers a blockchain protocol based on the Truffle development network to implement basic authentication and authorization operations as registration, login, user mapping and update of the system. We demonstrate how the Decentralized application(D-app) can be deployed as a simple and user-friendly web application and a rigorous case study in identity management domain.

2. LITERATURE SURVEY

2.1. Existing System

Nowadays, online marriage profiles matchmaking options are facing the issues of authenticity of the user's profiles. The oldest and effective profession for online marriages profiles includes the matchmaking using matrimony websites. The online matchmaking turns to be effective and popular among the younger generations who get to know the partners qualities and other essential things important for maintaining the secure and top profiles choices. Thus, with increasing use of the online matchmaking it leads to some serious issues leading to creation of fake profiles, disclosure of the user profiles to some websites over the internet. There are various matrimony websites currently available on the web and they have various measures for identity management of the user profile registered on their websites. Like the Bharat matrimony website uses the 6-point verification process for identifying the user to be authenticate user to login and proceed for checking other profiles which include document verification and access to social media accounts.

2.2. Major issues associated with existing system

1) Unauthenticated Profiles: As the online matchmaking is free to use for all users around the globe it leads to creation of the fake profiles for misuse which leads to profiles related authenticity problems [3]. The victims of those matches for fake profiles are

not able to find the difference in original and fake profiles.

2) Profiles Confidentiality: The profiles are created for various user around the country or world so the user never knows if the data/information that he/she provides is in safe hands. Thus, the problem of confidentiality plays important role in any system as it is lacking in existing online matchmaking systems [5].

3) Details of Past Life: It is not necessary that every user is new for profile creation some would have created their profiles and got their best matches. But still this people try to create new profiles with inaccurate information about their past life which is misleading information.

4) Inequality in profiles: Sometimes the users create some set of choices for their expected matches for different profiles around the matchmaking system [5]. But, sometimes the interest hits for this choice are in huge number so this creates a chaotic situation.

5) Misleading Profiles: Sometimes for the sake of getting the bright and the most imagined match by the user he/she tries to input the false information into the system [3]. Thus, every profiles user must be careful to find every detailed information and links before making the final decision.

6) Sudden Backout: Most of the times it is recorded that the users try to create profiles not out of excitement or willingness but just for fun. Such people backout from the given commitment thus genuine user becomes victims of such profiles. Thus, no user should fully trust any profiles until it is verified and matched correctly.

3. PROPOSED SYSTEM

Blockchain technology has the potential to help heal many of these online dating wounds. Blockchain technology is built on the idea of full transparency and immutability, two factors that can play a significant role in verifying user's identities, while maintaining the option of privacy and even allows for increased security [12]. To get rid of issues in existing system. we are proposing a system build with the blockchain technology to maintain the authenticity of profiles. This project deals with creation of block of data for different profiles and link them on the decentralized network such that each individual will have the copy of the his/her matched profiles/ Follow request profiles. This maintains the individual security of profiles and also fake profiles creation is terminated.

3.1. Blockchain Structure

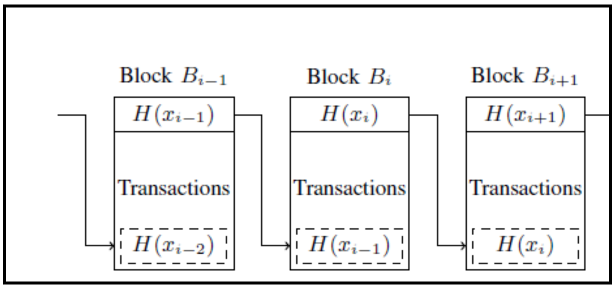


Fig 1. Blokchain Structure

A simple blockchain structure is represented in Fig.1 in which blocks or ledgers are linked in cryptographic manner using hash values.

It consists of hash pointers H(xi) used to reference other blocks while also providing means for integrity checking [1]. When consensus is achieved and given block is chosen, it will be inserted in the chain together with the transactions, which the node has validated.

This type may require successfully solving the Proof of Work (POW) depending on the type of blockchain in use [12].

In the same manner blockchain will keep the record of user immutable information and user's activity on the system as transactions.

3.2. Types of Blockchain

Initially, for powering Bitcoin, blockchain started as public permissionless technology. After that, many other types of blockchains have been developed [2]. There are three primary types of blockchain as follows.

1. Public blockchain:

Public blockchain is an open source, decentralized network. It allows anyone to participate as users, miners and developers. Since all the nodes verifies transaction and those are made public transaction [2], it is a secure network and transparent as well. Bitcoin and Ethereum are the primary examples of public blockchain.

2. Private blockchain:

Private blockchain is also known as permissioned blockchain. It is a partially decentralized network. Participant need consent to join the network. All the transactions are private in this network. This network is efficient as verification is done by only owner of the blockchain [2]. Hyperledger and R3 corda are the examples of private blockchain.

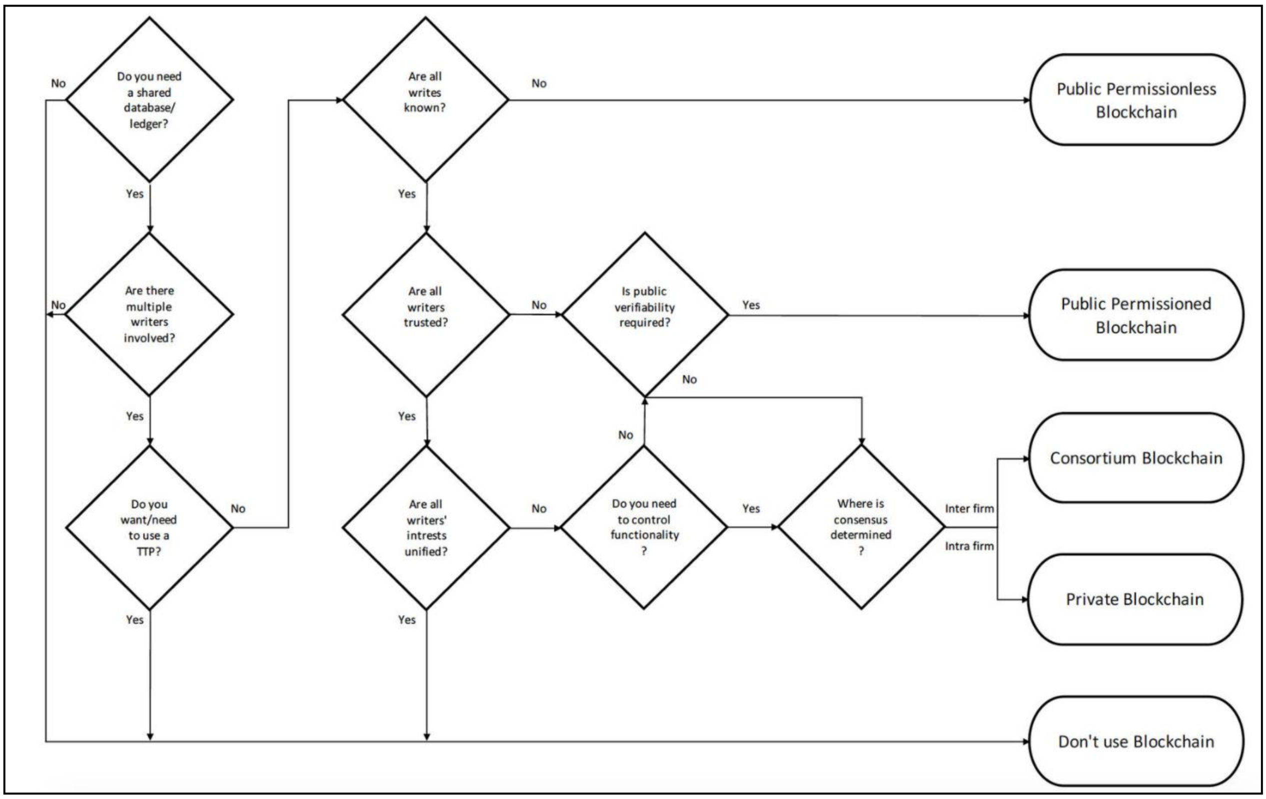

Do you need a shared database/ ledger?
No
Yes
Are there multiple writers involved?
No
Yes
Do you want/need to use a TTP?
No
Yes
Are all writes known?
No
Yes
Are all writers trusted?
No
Yes
Are all writers' intrests unified?
No
Yes
Is public verifiability required?
Yes
No
Do you need to control functionality ?
No
Yes
Where is consensus determined ?
Inter firm
Intra firm
Public Permissionless Blockchain
Public Permissioned Blockchain
Consortium Blockchain
Private Blockchain
Don't use Blockchain

Fig 2. Selecting a suitable Blockchain type

3. Hybrid blockchain:

The privacy benefits of a permissioned and private blockchain with the security and transparency benefits of a public blockchain together form as a hybrid blockchain. It is also a partially decentralized network. In this network, permissions to read/write, verify on the blockchains are controlled by few predefined nodes [2]. It is an efficient network as relatively lesser nodes verify the transactions Dragon chain is a example of hybrid blockchain

According to Fig.2, since we do not need the database and there are multiple writers involved in our system and also, we don't want to use third party tools we shall move to the blockchain technology.

Keeping the requirement and need of the system in mind, Public permission less blockchain is the right choice to implement the proposed system as users of the system are initially unknown for the system.

posed system

Following are the system features which makes proposed system stand out from the existing systems.

1. Decentralized and transparent: As system uses Ethereum Blockchain
2. Authentic Profiles: All user activities on the system are recorded
3. Membership plan:
Free Membership: User can browse all available profiles.
If any profile is liked by the user, he/she can send interest.

With free membership plan, chat features are restricted according to some parameters such as number of messages, number of users to chat, etc.

Paid Membership: User can browse all available profiles. If any profile is liked by the user, he/she can send interest

All the restrictions from free membership are relaxed in this membership plan and user get some additional features such as stickers, emojis, etc. User can view contact if provided by the opposite user. User can make his contact available to other users. User profile get the boost on browse profile feed. User queries will be answered by the admin

4. SYSTEM DESIGN

4.1. Architecture

The core architecture of the proposed system is shown in Fig.3. It consists of a client-side user interface (UI), blockchain, and Database (DB).

In simple scenario, through the UI user interacts with the system to perform the desired actions. The UI is web applications that communicated with the database and blockchain to perform the desired functions.

Client-side UI consists of various nodes such as register, login and dashboard modules. Further dashboard is divided into different nodes so as to perform activities desired by user.

Web app and Blockchain communicates using the smart contract and web3 JS. Logs for different user activities are stored in the blocks with required data and timestamp. Basic information about the user which is immutable is stored in the blockchain such as name, DOB. Information about the user mapping is stored on the blockchain as well as it need to be authenticated and secure activity.

Database is any sequel database, for example MySQL. Web app and DB will communicate based on request and response. It will store mutable information about the user such as username, password and other details. User chat will be stored as well in the DB.

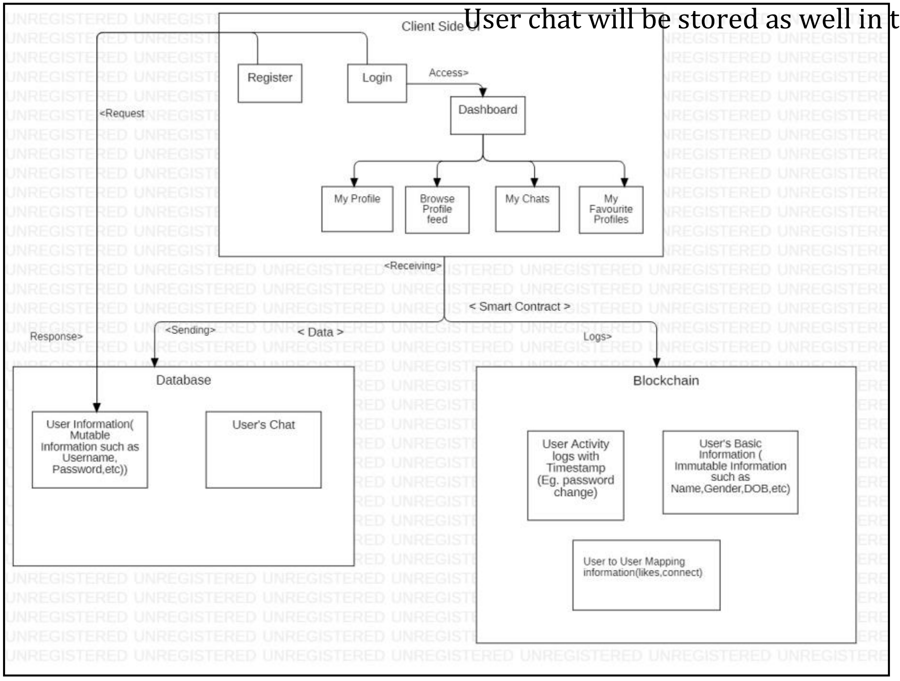

Client Side UI
Register
Login
Access>
Dashboard
<Request
My Profile
Browse Profile feed
My Chats
My Favourite Profiles
<Receiving>
< Smart Contract >
<Sending>
< Data >
Response>
Logs>
Database
User Information(Mutable Information such as Username, Password,etc))
User's Chat
Blockchain
User Activity logs with Timestamp (Eg. password change)
User's Basic Information (Immutable Information such as Name,Gender,DOB,etc)
User to User Mapping information(likes,connect)

Fig 3. Architecture Diagram

4.2 Information Architecture

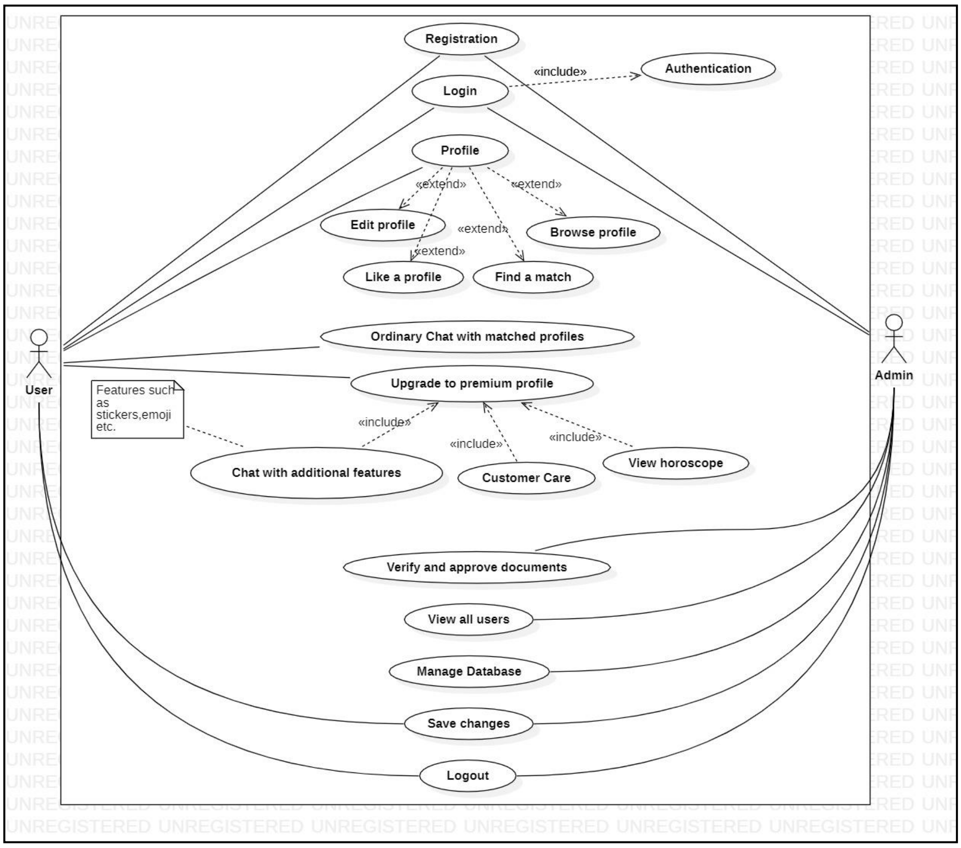


Fig 4. Information Architecture Diagram

Information Architecture (IA) means defining the different types of users for your system and what each user type can do in the system. That is defining the different actions he can take.

This system has two users namely,

- User
- Admin

Fig.4 represents the IA for the proposed system which includes two users. Depending upon the membership, user can perform all the actions such as registration, login, browsing other profiles and chatting with the other users.

If user has free membership plan, he/ she will be able to access all the basic features of the system right from the registration to chat feature. But as mentioned above in the system features, user will not get access to some additional things such as use of stickers and emojis. If user has paid membership plan, he/she will get access to all additional features such as customer care, view horoscope and use of stickers, emojis while chatting. Admin can perform actions like view all users, manage database. Also, admin can verify the documents uploaded by the user in verification process.

5. SYSTEM IMPLEMENTATION

We are developing a proposed system which will used by the users to find his/her perfect match. System implementation is further categorized into following.

5.1. Front End Development

1. React JS: For building user interfaces or UI components, React JS is used which is an open- source framework and front-end JS library. The screens or web pages are developed using react Js. It provides reusability of the components.

5.2. Ethereum Network Development (Blockchain)

1. Truffle development network: Truffle is a Ethereum development environment, testing framework for blockchain and uses Ethereum virtual machine (EVM) [17]. It can be called as local blockchain and provides 10 accounts with account address, 100 ethers and its private keys. Different smart contracts for activities such as registration, like a user are deployed using truffle commands on the network. For any transactions on the system, some amount in the form of ethers is deducted from the user account.

2. Metamask: Metamask is a cryptocurrency wallet and gateway to Decentralized app (DApp) [14]. Accounts provided by the truffle development are imported in the metamask to use them whenever any transactions on the system ask for ethers.

3. Smart contract: A set of agreed promises or rules including protocols specifying how the parties deliver on these promises called as Smart contract. It is converted to a computer code, stored and replicated in the blockchain [1]. We are using Solidity programming language to write the smart contracts. For every activity on the system there is smart contract deployed on the truffle network. Whenever user perform any activity contract gets initiated and respective data gets stored in the blockchain.

4. Web3 JS:

Web3 JS is a Ethereum JavaScript API which is a collection of libraries which allows to communicate with the local Ethereum node using HTTP, IPC or Websocket [19],[20]. In this proposed system our local node is truffle network and Web3 JS will allow our Webapp to communicate with the truffle network using smart contract.

5.3. Backend Development

1. Node JS: It is a backend JavaScript runtime environment which is an open source and executes outside the browser.It will help Web app to communicate with DB.

2. MySQL: It is a sequel database which will store the mutable data such as username and password. It will also keep the record of user chats.

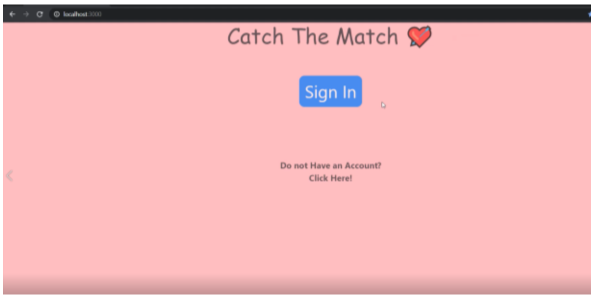
6. RESULTS AND DISCUSSION

6.1. Discussion

- Comparison of Existing System and Proposed System

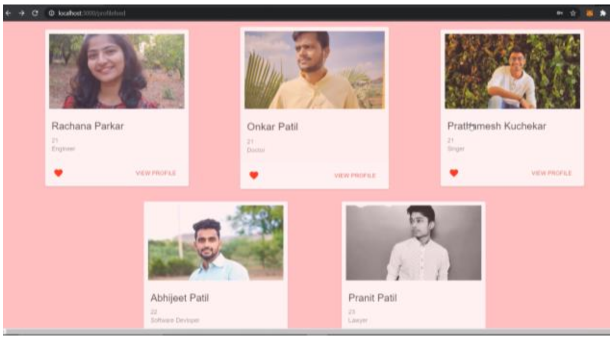
Existing System	Proposed System
Centralized	Decentralized
Question of authenticity	Authentic Profiles
Question of confidentiality	Transparent activities
Data is vanished once deleted	Cannot delete the immutable data

6.2. Results



Do not Have an Account?
Click Here!

Fig 5. Landing Page



Rachana Parkar
21
Engineer

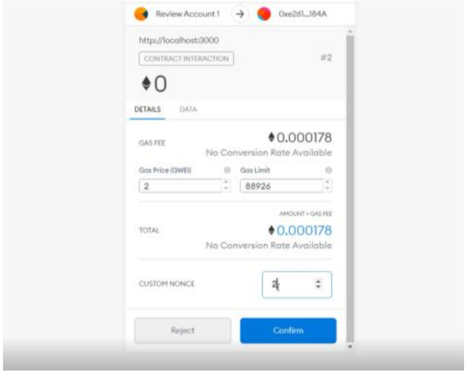
Onkar Patil
21
Doctor

Prathamesh Kuchekar
21
Singer

Abhijeet Patil
22
Software Developer

Pranit Patil
23
Lawyer

Fig 6. User Dashboard



Review Account 1 → 0xe261...184A
http://localhost:3000
CONTRACT INTERACTION #2
0
GAS FEE 0.000178
No Conversion Rate Available
Gas Price (GWEI): 2
Gas Limit: 88926
AMOUNT + GAS FEE
TOTAL 0.000178
No Conversion Rate Available
CUSTOM NONCE: 2

Fig 7. Recording user activity as transaction through metamask

7. CONCLUSION

In this paper we proposed a system for Matrimony Website using blockchain for tracking authenticity of profiles. A prototype based on local blockchain called as truffle development network was made to demonstrate the usability of such a system. This system offers immutability of profiles if user saves a profile as a ledger or a block in the blockchain then we cannot delete the profile. Thus, history of the user will be available in the blockchain. It also provides authenticity once the user profile is saved in the ledger, it is not possible to create another profile with the same user information (mainly same account address) because, blockchain creates the hash value of each block. Hacking is also eliminated in this system since blockchain is the decentralized system, single change in the block can differ the hash value of the block. It confirms that, in decentralized, efficient and secure manner, identity and access management can be achieved.

REFERENCES

[1] https://www.researchgate.net/publication/328313216 Identity and Access Management with Blockchain in Electronic Healthcare Records

[2] https://devopedia.org/types-of-blockchains

[3] https://www.researchgate.net/publication/333918869 Analysis of Identity Management Systems Using Blockchain Technology

[4] Paul Dunphy and Fabien A. P. Petitcolas,Innovation Centre,VASCO Data Security{paul.dunphy,fabien.petitcolas}@vasco.com A First Look at Identity Management Schemes on the Blockchain.

[5] Received: 6 June 2019; Accepted: 17 July 2019; Published: 24 July 2019 DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network.

[6] https://www.coursera.org/specializations/blockchain

[7] https://coursetro.com/courses/20/Developing-Ethereum-Smart-Contracts-for-Beginners

[8] Identity and access management with blockchain in electronic healthcare system by Tomas Mikula And Rune jacabson.

[9] A blockchain identity management system to secure personal data sharing in network by Jamila Kaseem and SarwarSayeed.

[10] A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data MIT Media Lab, Beth Israel Deaconess Medical Center - August 2016

[11] Blockchain technology for government by Dave Bryson and DavePenny

[12] Blockchain: A New Digital Revolution The Parliament Magazine - November 2018

[13] Blockchains: How They Work and Why They'll Change the World by Morgen E. Peck

[14] https://www.toptal.com/ethereum/one-click-login-flows-a-metamask-tutorial

[15] https://www.tutorialspoint.com/solidity/index.htm

[16] https://www.w3schools.com/nodejs/nodejs_intro.asp

[17] Research on truffles: Scientific journals analysis by Dorota Hilszczanska

[18] Using the web3.js APIs by Wei-Meng Lee

[19] https://medium.com/coinmonks/interacting-with-ethereum-smart-contracts-through-web3-js-e0efad17977

[20] https://blog.infura.io/ethereum-javascript-libraries-web3-js-vs-ethers-js-part-i/

[21] https://www.guru99.com/introduction-to-mysql-workbench.html