Project Id: 2016CSEPID056

Project Report
on

Blockchain-Blockcerts based Birth/Death Certificate Registration and Validation

Submitted In Partial Fulfillment of the

Requirement For the Degree of

Bachelor of Technology

In

Computer Science and Engineering

By

NITESH SHARMA (1629010105)
MOHAMMAD AFZAL (1629010089)

Under the Supervision of
Ms. Ankita Dixit

(Assistant Professor)

Department of Computer Science & Engineering
ABES INSTITUTE OF TECHNOLOGY, GHAZIABAD

AFFILIATED TO
Dr A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, UTTAR PRADESH, LUCKNOW
(May-2020)

DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature: Nitesh Sharma
Name: Nitesh Sharma
Roll No.: 1629010105
Date: 28 April, 2020

Signature: Mohammad Afzal
Name: Mohammad Afzal
Roll No.: 1629010089
Date: 28 April, 2020

CERTIFICATE

This is to certify that Project Report entitled "Blockchain-Blockcerts based Birth/Death Certificate Registration and Validation" which is submitted by Nitesh Sharma and Mohammad Afzal

in partial fulfillment of the requirement for the award of degree B. Tech. in Department of

Computer Science and Engineering of Dr. A.P.J. Abdul Kalam Technical University, is a record of the candidate own work carried out by him under my/our supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date: 28 April, 2020

Supervisor:
Ms. Ankita Dixit
Assistant Professor, Department of Computer Science and Engineering
ankita.dixit@abesit.in

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B. Tech Project undertaken during B. Tech. Final Year. We owe special debt of gratitude to Asst. Professor Ankita Dixit, Department of Computer Science & Engineering, ABES Institute of Technology, Ghaziabad for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen light of the day.

We also take the opportunity to acknowledge the contribution of Dr. Rizwan Khan, Head, Department of Computer Science & Engineering, ABES Institute of Technology, Ghaziabad for his full support and assistance during the development of the project.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Signature: Nitesh Sharma
Name: Nitesh Sharma
Roll No.: 1629010105
Date: 28 April, 2020

Signature: Mohammad Afzal
Name: Mohammad Afzal
Roll No.: 1629010089
Date: 28 April, 2020

ABSTRACT

As we know that Birth/Death Certificates are very essential documents. Birth Certificate can be used as proof of an individual's age, for academics, for jobs and can be used as an identity for various government documents (Passport, Driving License, Voter-ID, etc.). Likewise, Death Certificates can be used by the family of deceased to inherit property, to claim insurance benefits and used by the government to maintain population statistics. In the current scenario, due to the complex procedure of applying and getting a certificate, nearly half of the world's population does not have a birth certificate. Also, authentication of a valid certificate is a laborious task. At the same time, due to the presence of hard copy, missing certificate becomes a crucial problem and re-issuing of that certificate is a hectic process. Presently, the digital certificate is a way to tackle the problem of missing certificates still it is not sufficient as it can tamper easily.

Therefore, the objective of this paper is to give the solution to issue Birth/Death certificates and validation of certificates using Blockcerts which is based on Blockchain Technology. Blockcerts is used for issuing and verifying a blockchain-based formal transaction. Blockchain is a shared distributed, decentralized database system used to store information and this information cannot tamper easily. It also provides security services like confidentiality, authentication, integrity and access control list of data.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Background of Block chain

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The PartTime Parliament to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System, which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto's paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications). Bitcoin was just the first of many blockchain applications [1].

In year 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". This paper described a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept. Now word cryptocurrencies are the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions-as against those systems where the transactions are channeled through a centralized trusted entity [2].

The author of the first paper wanted to remain anonymous and hence no one knows Satoshi

Nakamoto to this day. A few months later, an open source program implementing the new protocol was released that began with the Genesis block of 50 coins. Anyone can install this open source program and become part of the bitcoin peer-to-peer network. It has grown in popularity since then. [2]

Many electronic cash schemes existed prior to Bitcoin (e.g., ecash and NetCash), but none of them achieved widespread use. The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party. It also enabled the issuance of new cryptocurrency in a defined manner to those users who manage to publish new blocks and maintain copies of the ledger; such users are called miners in Bitcoin. The automated payment of the miners enabled distributed administration of the system without the need to organize. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain.

In Bitcoin, the blockchain enabled users to be pseudonymous. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible. This has effectively enabled Bitcoin to offer pseudo-anonymity because accounts can be created without any identification or authorization process (such processes are typically required by Know-Your-Customer (KYC) laws) [1].

1.2 Introduction of Blockchain

A blockchain is a digital ledger created to capture transactions conducted among various parties in a network. It is a peer-to-peer, Internet-based distributed ledger which includes all transactions since its creation. All participants (i.e., individuals or businesses) using the shared database are “nodes” connected to the blockchain, each maintaining an identical copy of the ledger. Every entry into a blockchain is a transaction that represents an exchange of value between participants (i.e., a digital asset that represents rights, obligations or ownership). In practice, many different types of blockchains are being developed and tested. However, most blockchains follow this general framework and approach [3].

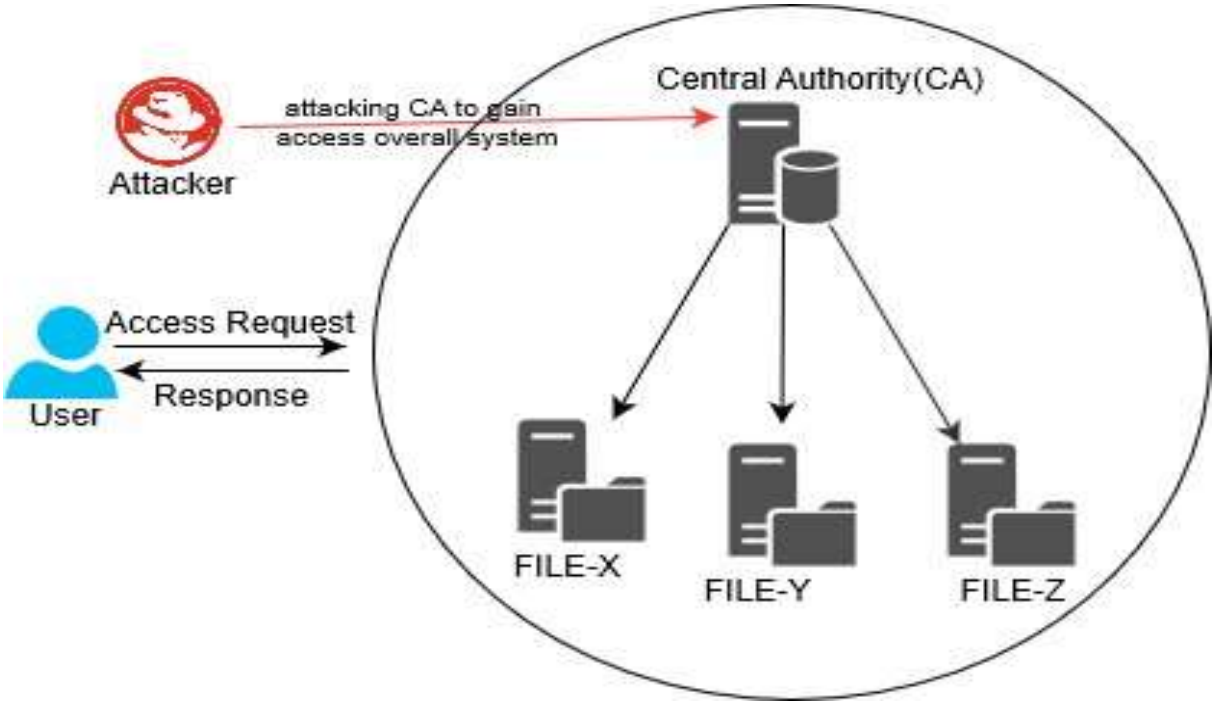


Figure 1: Tampering in Centralized System

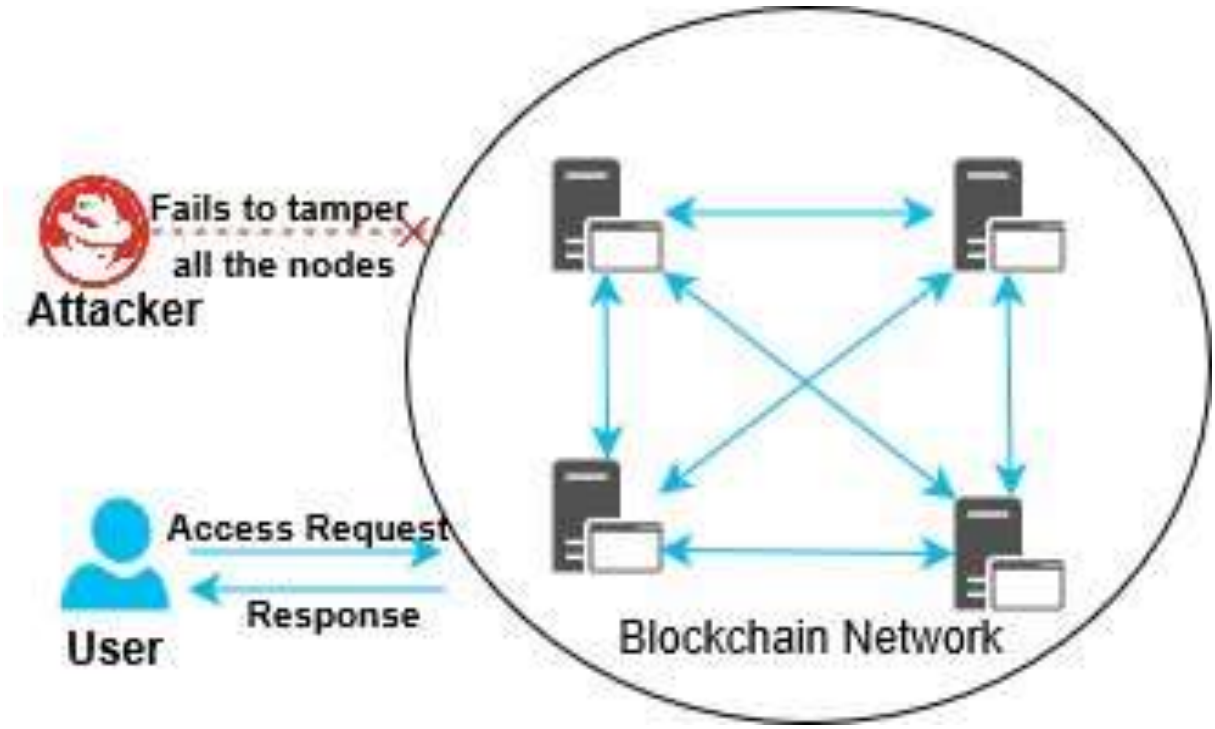


Figure 2: Tampering in Decentralized System

When one participant wants to send value to another, all the other nodes in the network communicate with each other using a pre-determined mechanism to check that the new transaction is valid. This mechanism is referred to as a consensus algorithm. Once a

transaction has been accepted by the network, all copies of the ledger are updated with the new information. Multiple transactions are usually combined into a “block” that is added to the ledger. Each block contains information that refers back to previous blocks and thus all blocks in the chain link together in the distributed identical copies.

Participating nodes can add new, time-stamped transactions, but participants cannot delete or alter the entries once they have been validated and accepted by the network. If a node modified a previous block, it would not sync with the rest of the network and would be excluded from the blockchain. A properly functioning blockchain is thus immutable despite lacking a central administrator [3].

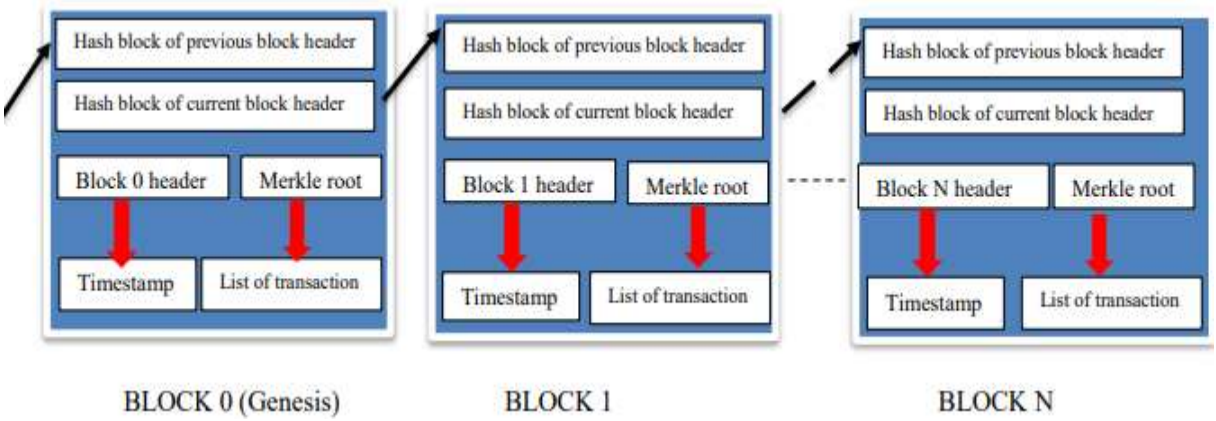


Figure 1: Structure of Blockchain

In the simplest terms, Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. You can also think of it as a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it [4].

Each transaction on a blockchain is secured with a digital signature that proves its authenticity. Due to the use of encryption and digital signatures, the data stored on the blockchain is tamper-proof and cannot be changed.

Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party.

In order to understand blockchain better, consider an example where you are looking for an option to send some money to your friend who lives in a different location. A general option that you can normally use can be a bank or via a payment transfer application like PayPal or Paytm. This option involves third parties in order to process the transaction due to which an extra amount of your money is deducted as transferring fee. Moreover, in cases like these, you cannot ensure the security of your money as it is highly possible that a hacker might disrupt the network and steal your money. In both the cases, it is the customer who suffers. This is where Blockchain comes in [4].

Instead of using a bank for transferring money, if we use a blockchain in such cases, the process becomes much easier and secure. There is no extra fee involved as the funds are directly processed by you thus, eliminating the need for a third party. Moreover, the blockchain database is decentralized and is not limited to any single location meaning that all the information and records kept on the blockchain are public and decentralized. Since the information is not stored in a single place, there is no chance of corruption of the information by any hacker [4].

1.3 Structure of Block

Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the blockchain network. The chosen nodes may be non-publishing full nodes as well as publishing nodes. The submitted transactions are then propagated to the other nodes in the network, but this by itself does not place the transaction in the blockchain. For many blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node [1].

Transactions are added to the blockchain when a publishing node publishes a block. A block contains a block header and block data. The block header contains metadata for this block. The block data contains a list of validated and authentic transactions which have been submitted to the blockchain network. Validity and authenticity are ensured by checking that the transaction is correctly formatted and that the providers of digital assets in each

transaction (listed in the transaction's 'input' values) have each cryptographically signed the transaction. This verifies that the providers of digital assets for a transaction had access to the private key which could sign over the available digital assets. The other full nodes will check the validity and authenticity of all transactions in a published block and will not accept a block if it contains invalid transactions.

It should be noted that every blockchain implementation can define its own data fields; however, many blockchain implementations utilize data fields like the following [1]:

- **Block Header**
  - The block number, also known as block height in some blockchain networks.
  - The previous block header's hash value.
  - A hash representation of the block data (different methods can be used to accomplish this, such as a generating a Merkle tree (defined in Appendix B), and storing the root hash, or by utilizing a hash of all the combined block data).
  - A timestamp.
  - The size of the block.
  - The nonce value. For blockchain networks which utilize mining, this is a number which is manipulated by the publishing node to solve the hash puzzle (see Section 4.1 for details). Other blockchain networks may or may not include it or use it for another purpose other than solving a hash puzzle.

- **Block Data**
  - A list of transactions and ledger events included within the block.
  - Other data may be present.

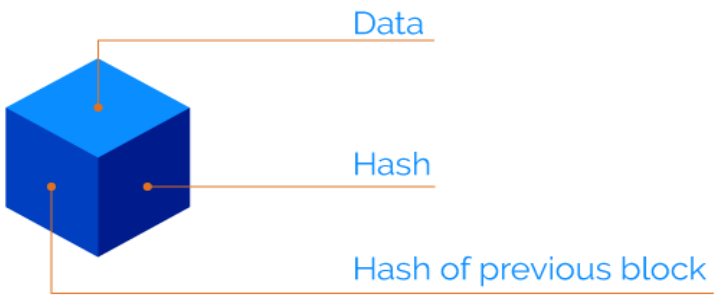


Figure 2: Simplified Structure of Block

1.4 Merkle Root and Merkle Tree

A Merkle root is the hash of all the hashes of all the transactions that are part of a block in a blockchain network.

- A Merkle root is a simple mathematical way to verify the data on a Merkle tree.
- Merkle roots are used in cryptocurrency to make sure data blocks passed between peers on a peer-to-peer network are whole, undamaged, and unaltered.
- Merkle roots are central to the computation required to maintain cryptocurrencies like bitcoin and ether.

Understanding a Merkle Root

A blockchain is comprised of various blocks that are linked with one another (hence the name blockchain). A hash tree, or the Merkle tree, encodes the blockchain data in an efficient and secure manner. It enables the quick verification of blockchain data, as well as quick movement of large amounts of data from one computer node to the other on the peer-to-peer blockchain network.

Every transaction occurring on the blockchain network has a hash associated with it. However, these hashes are not stored in a sequential order on the block, rather in the form of a tree-like structure such that each hash is linked to its parent following a parent-child tree-like relation.

Since there are numerous transactions stored on a particular block, all the transaction hashes in the block are also hashed, which results in a Merkle root.

For example, consider a seven-transaction block. At the lowest level (called the leaf-level), there will be four transaction hashes. At the level one above the leaf-level, there will be two transaction hashes, each of which will connect to two hashes that are below them at the leaf level. At the top (level two), there will be the last transaction hash called the root, and it will connect to the two hashes below it (at level one).

Effectively, you get an upside-down binary tree, with each node of the tree connecting to only two nodes below it (hence the name "binary tree"). It has one root hash at the top, which connects to two hashes at level one, each of which again connects to the two hashes at level three (leaf-level), and the structure continues depending upon the number of transaction hashes.

The hashing starts at the lowest level (leaf-level) nodes, and all four hashes are included in the hash of nodes that are linked to it at level one. Similarly, hashing continues at level one, which leads to hashes of hashes reaching to higher levels, until it reaches the single top root hash.

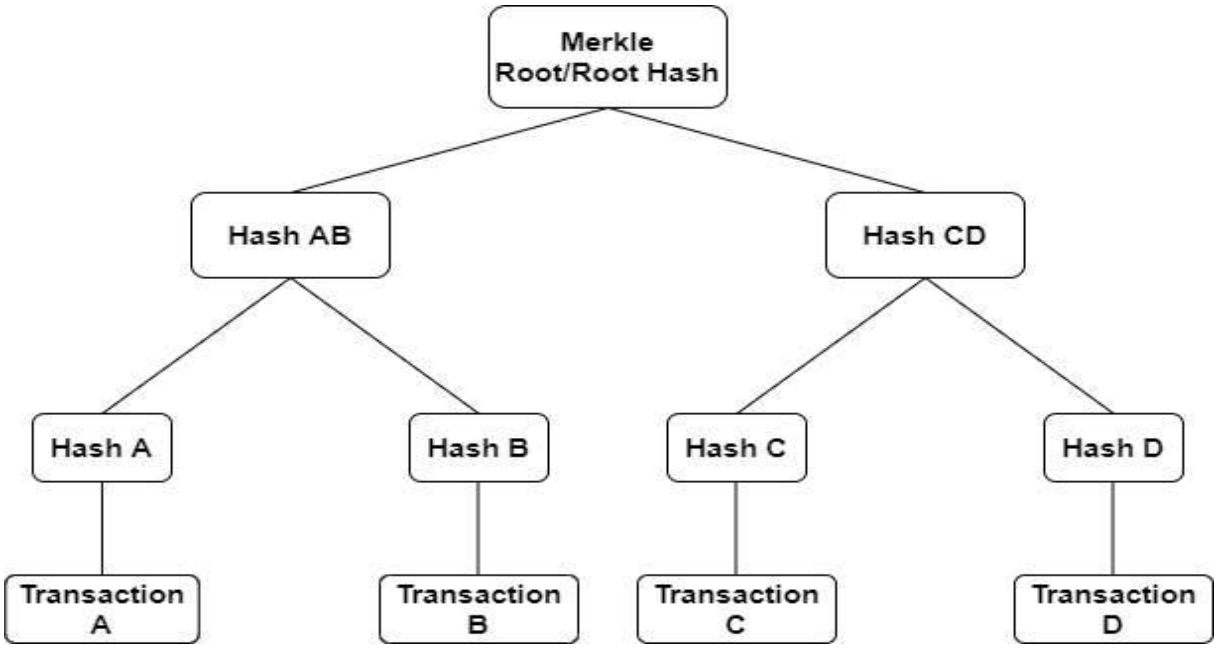


Figure 3: An Example of Merkle Tree

This root hash is called the Merkle root, and due to the tree-like linkage of hashes, it contains all the information about every single transaction hash that exists on the block. It offers a single-point hash value that enables validating everything present on that block.

Merkle Tree

Merkle trees are a fundamental part of blockchain technology. A Merkle tree is a structure

that allows for efficient and secure verification of content in a large body of data. This structure helps verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle trees.

How do Merkle trees work?

A Merkle tree summarizes all the transactions in a block by producing a digital fingerprint of the entire set of transactions, thereby enabling a user to verify whether or not a transaction is included in a block. Merkle trees are created by repeatedly hashing pairs of nodes until there is only one hash left (this hash is called the Root Hash, or the Merkle Root). They are constructed from the bottom up, from hashes of individual transactions (known as Transaction IDs).

Each leaf node is a hash of transactional data, and each non-leaf node is a hash of its previous hashes. Merkle trees are binary and therefore require an even number of leaf nodes. If the number of transactions is odd, the last hash will be duplicated once to create an even number of leaf nodes [5].

1.5 Characteristics of Blockchain

- **Decentralized Technology:** In centralized transactions model, all the transaction needs to be permitted by the single central body whereas in blockchain network the transactions are performed in Peer-to-Peer manner that's mean two nodes communicate directly with each other as shown in Fig. 1 and Fig.2 [6].
- **Cannot be corrupted:** In blockchain network there are several nodes and each node have a replica of the valid ledger. The new transaction can only be added when the majority of the nodes will be agreed on that transaction. In this way, we can achieve a corruption free network and avoid invalid transactions [6].
- **Distributed Ledger:** In the blockchain network, all the resources are distributed among all sites of the blockchain, there is no single central database to store the resources [7].
- **Enhance Security:** Each block in the blockchain have a hash value and also contains

the hash value of the previous block, if an attacker wants to tamper the block then he has to tamper all the block which is quite impossible. Another aspect of enhancing security in the blockchain is asymmetric cryptography.

- **Consensus:** In the blockchain network the set of nodes are responsible for the addition of new block in the blockchain, these set of nodes are selected based on various consensus algorithm such as PoW, PoS, MoT, etc. As explained in Table 1[8].

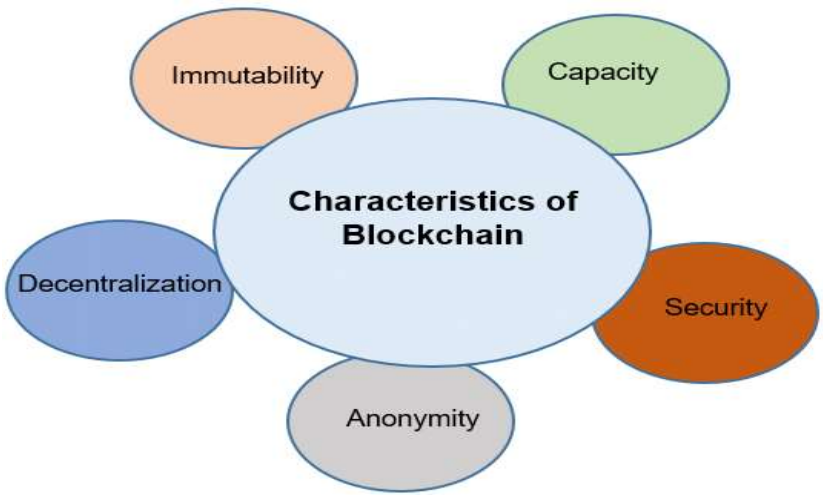


Figure 4: Characteristics of Blockchain

1.6 Mining a Block in Blockchain

Mining is the process of creating blocks that will be attached to the database. In some of the blockchain applications, such as in Bitcoin, the miner who creates the first valid block is rewarded. This reward is given by the system and is generally in terms of money for financial applications. Mining is one of the critical concepts in the blockchain technology. It allows nodes to create blocks which will be validated by others as well. If the new block is found as valid, it is attached to the blockchain database. Nodes that try to create blocks are called *"mining nodes."* The mining nodes race to validate the transactions and create a new

block as fast as they can to win the reward [9].

Several approaches exist to decide which miner wins, including proof of work (PoW), proof of Stake (PoS), Proof of Space (Popsicle), Proof of Importance (PoI), Measure of Trust (MoT), minimum block hash, and Practical Byzantine Fault Tolerance (PBFT). In the following, we summarize these major mining approaches (see also Table I).

- **Proof of Work:** PoW is the mining technique used in Bitcoin and is currently used by many other blockchain technologies. It requires the mining nodes to solve a hard-mathematical puzzle that is changed frequently and has been agreed by all the miners. Once a node validates the transactions and solves the puzzle, the block is submitted to the blockchain network. Other mining nodes validate the block to make sure that the submitter is not falsifying. Once it is agreed among the miners that the block is legit, it will be added to the blockchain and the submitter will be rewarded. The agreement here is based on a majority consensus. Thus, it is difficult to fake unless the attackers compromise more than 50 percent of the mining nodes. The problem with this approach is that high computational power is wasted in solving the mathematical puzzle.

- **Proof of Stake:** Unlike PoW, PoS does not require the mining nodes to solve a computationally expensive mathematical puzzle. Instead, the next block creator or miner is chosen in a pseudo-random way. The chance of a node being chosen to create the new block depends on the node's wealth or stake. In other words, the more money a node has, the higher its chances to mine a block. The native version of PoS does not award the miner; however, the extended versions award and punish the creators based on their performance. Selection based on the wealthiest account may result in a single account handling all the creations; hence, it may lead to an unfair distribution or even centralization. Therefore, a randomized node selection and a coin age-based selection have been proposed. In coin age-based method, the users that have not created any block for the past 30 days are considered for mining [9].

- **Proof of Space:** PoSpace is similar to PoW except that the puzzle requires a lot of storage. A miner proves its ability to create a new block by allocating the required

storage space to perform mining. In other words, instead of having a high computational capability, the mining node needs to have a high storage capability. Several theoretical and practical implementations of PoSpace have been released; however, the required high memory space is a challenge similar to the computation challenge of PoW.

- **Proof of Importance:** PoI is a mining technique that calculates the significance of an individual node based on the transaction amount and the balance of that node. It assigns a priority with a hash calculation to the more significant nodes. Further, the node with the highest priority is chosen for the next block creation.

- **Measure of Trust:** Another way to perform mining is to use dynamic trust measurements and select the node with the highest trust level as the block initiator. The trustworthiness is based on the nodes' behaviors; therefore, good behaving nodes that follow the protocols are rewarded. More specifically, the trustworthiness could be formulated as the expected value of the node's behavior in the future. This, the trustworthiness is approximated by the history of good and bad actions that the node has taken so far. The MoT approach could be subject to malicious attacks if a specific node plans to increase its trustworthiness for several iterations in order to attack the network later.

- **Minimum Block Hash:** In this, the miner is chosen randomly and not based on its resources. The system selects the miners based on a generated minimum hash value across the entire network. Thus, the selection of the next miner is randomized and the probability of selecting the same miner is low. This approach was implemented on a modified Bitcoin network and it was shown to offer energy savings for mining. However, it has not been adopted by the Bitcoin community.

- **Practical Byzantine Fault Tolerance:** Unlike others, PBFT is a consensus approach that does not include any type of resources but utilizes the blockchain consensus based on the Byzantine fault tolerance approach. In this approach, first, a leader is selected and agreed among the nodes. The leader decides on the transactions' validation and publishes a block to all the nodes in the blockchain network. A

transaction is committed to a new block only if two-thirds of the mining nodes verify its correctness. The leader changes frequently; therefore, the approach is not considered as centralized. PBFT has been shown to be faster than other methods; however, it suffers from scalability issues due to the resulting communication overhead [9].

TABLE 1. Comparison between Different Mining Techniques

Mining Technique	Assets Required	Application	Reward-based
Proof of Work	High computational Power	Bitcoin	Yes
Proof of Stake	Wealth or Stake	Ethereum	No
Proof of Space	High Storage	SpaceMint	Yes
Proof of Importance	Node Importance	Nem	Yes
Measure of Trust	Trust Value	Not implemented	Yes
Minimum hash block	Minimum Hash Value	Bitcoin (modified)	Yes

1.7 Working of Blockchain

In figure 7, the working of blockchain is explained. There are mainly six steps in the overall process.

In first step, the user will provide the required details. In second step, a block will be created which contains relevant information regarding the transaction. In third step, the block will be

broadcasted to every node in the blockchain. Then, in fourth step, all the node will validate the details provided by the user in the first step. After validation, new block will be added to the existing growing blockchain. Hence, the transaction is completed in the last step [10].

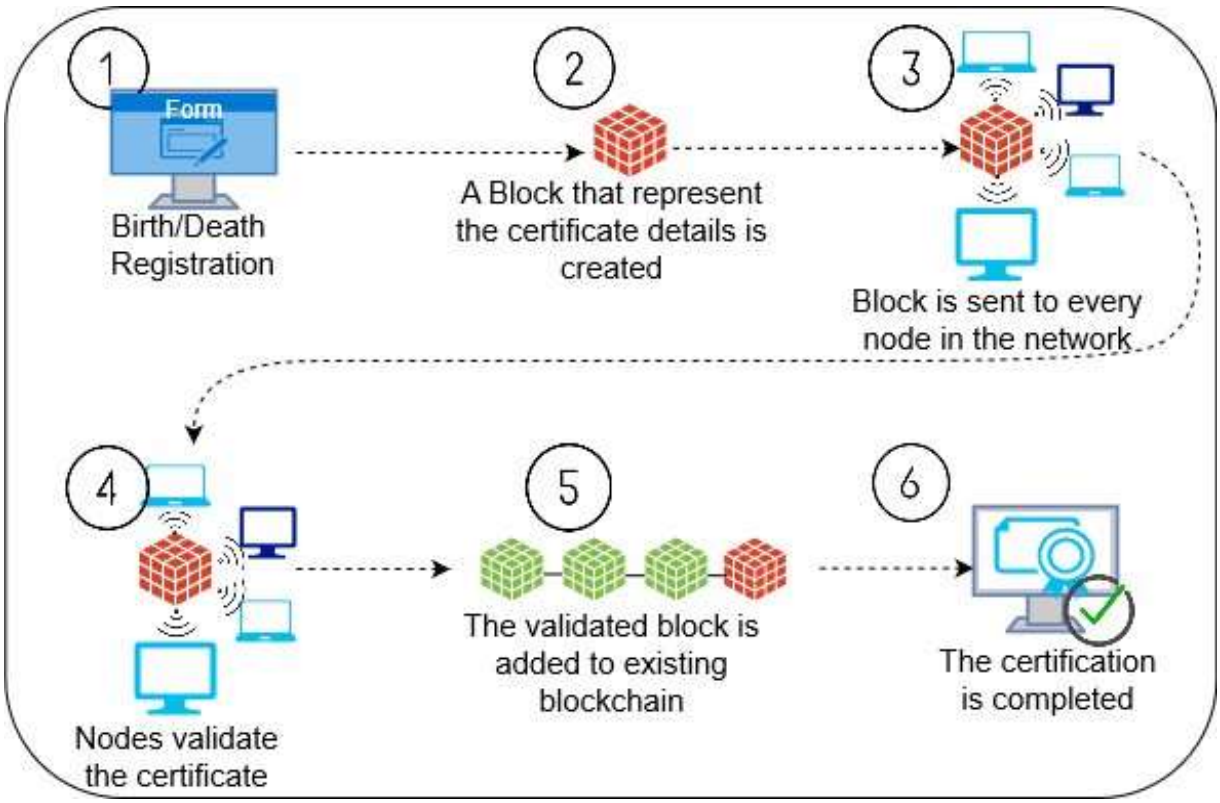


Figure 5 Working of blockchain technology

1.8 PUBLIC/PRIVATE KEY CRYPTOGRAPGY IN BLOCKCHAIN TECHNOLOGY

Cryptography is a method of securing data confidentiality from unauthorized persons. For cryptography, we have to perform the following operation: Encryption and Decryption. Blockchain uses public key cryptography techniques to secure transactions, preserve user privacy and maintains data integrity. The public key cryptography uses two types of key: a public key and private key. A public key is distributed publicly over a network and can be used by anyone in the network whereas the private key is kept confidential by the user. Every user has its pair of keys (Public key and its corresponding Private key) [11].

Encryption in Blockchain Technology

Encryption is a technique in which the normal text is transformed into an unreadable form. In Blockchain, we use a hashing encryption algorithm to encrypt the information. So, if any malicious user tries to access the information then the information will be of no use as the information is in the encrypted form. The hashing encryption algorithm uses the public key to encrypt the information that can only be decrypted using the corresponding private key. The most common applications of blockchain technology are Bitcoin and Ethereum which are using SHA256 and KECCAK256 encryption algorithm respectively [11].

Digital Signature

The digital signature is used to verify the authenticity of a digital document. It is used to prove that the specific information belongs to the sender who has made the digital signature [6]. It involves two parts, the signing part, and the verification part. In signing part, the sender will sign the document using its private key. The digitally signed document will be broadcasted over the whole blockchain network which is accessible by everyone. In the second part, the receiver can verify a digitally signed document by using the sender's public key [6].

Decryption in Blockchain Technology

Decryption is a technique in which encrypted information is taken and converted into its original form by using a corresponding private key.

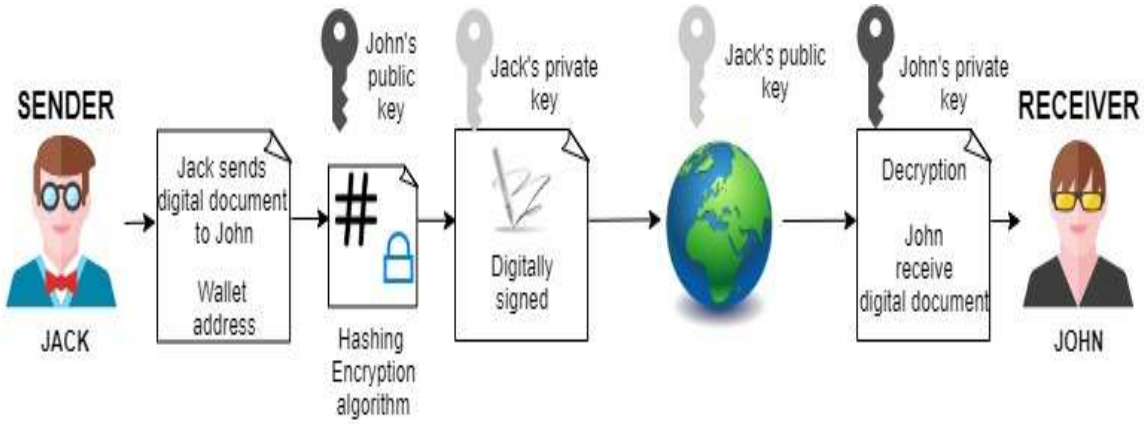


Figure 8: An example of public/private key cryptography

Let's take an example of Public/Private key cryptography as shown in Fig. 8. In this figure, Jack wants to send a digital document to John. Therefore, Jack will use John's public key to encrypt the digital document and digitally sign the document by using its private key. Then

Jack sends a digitally signed and encrypted document to John over the blockchain network. In between, no one can read the document because it is in the encrypted form. Now, John will use its private key to decrypt the encrypted document and validate the same document by using Jack's public key.

1.9 REAL EXAMPLES OF BLOCKCHAIN TECHNOLOGY IN PRACTICE

Entertainment

- **KickCity**—Platform for event organizers that enables them to pay only for what they get, and rewards community members by sharing those events. Their products generate around $50k monthly with more than 70k users and 300 event hosts.
- **B2Expand**—Based on the Ethereum blockchain they create cross-gaming video games. Their first video game "Beyond the Void" got into Ubisoft's startup program and they're the first gaming company on Steam with a crypto economy.
- **Spotify**—When Spotify acquired blockchain startup Mediachain Labs it was to help develop solutions via a decentralized database to better connect artists and licensing agreements with the tracks on Spotify's service.
- **Guts**—A transparent ticketing ecosystem that uses blockchain technology to eliminate ticket fraud and the secondary ticket market [12].

Social Engagement

- **Matchpool**—"Matchmakers" are rewarded for making successful matches whether it's dating to freelancing to Uber and Airbnb.

Retail

- **Warranteer**—A blockchain application that allows consumers to easily access info regarding the products they purchased and get service in the case of product malfunction.

- **Blockpoint**—Simplifies the creation of payment systems and allows mobile wallet, loyalty program, gift cards and other point-of-sale functionality.
- **Loyyal**—Powered by blockchain and smart contract technology, this loyalty and rewards platform creates more customized programs that even allow for multi-branded rewards.

Exotic Cars

- **Bitcar**—Fractionalized ownership of collector cars made possible by a BitCar token.

Supply chains and logistics

- **IBM Blockchain**—Knowing the status and condition of every product on your supply chain from raw materials to distribution is critical. Blockchain for supply chains allows transparency with a shared record of ownership and location of parts and products in real time.
- **Food industry**—The food industry's complex network from farmers to grocers makes tracking down food-borne illnesses challenging. Blockchain can improve the transparency and efficiency of finding out what food might be contaminated and where throughout the supply chain.
- **Provenance**—Consumers are increasingly demanding transparency regarding the products they purchase and consume to ensure the sourcing of materials and production of products adheres to their individual values. Provenance uses blockchain to provide chain-of-custody and certification of supply chains.
- **Blockverify**—With a claim to "introduce transparency to supply chains," Blockverify focuses on anti-counterfeit solutions using blockchain to verify counterfeit products, diverted goods, stolen merchandise and fraudulent transactions.
- **OriginTrail**—Already in use in the food industry, more applications are planned for OriginTrail, a platform that lets consumers know where their purchases came from and how they were produced.
- **De Beers**—De Beers mines, trades and markets more than 30% of the world's supply of diamonds. The company plans to use a blockchain ledger for tracing diamonds from the mine to the customer purchase. This transparency will help the industry and

anybody who wishes to verify, confirm diamonds are free from conflict. also plans to use blockchain in its supply process of emeralds, rubies and other precious stones [12].

Insurance

- **Accenture**—With goals to boost efficiency and productivity within the insurance industry, Accenture builds blockchain solutions for its insurance clients. They translate key insurance industry processes into blockchain-ready procedures that embed trust into the system.
- **Proof of insurance**—Nationwide insurance company is currently testing a blockchain solution to provide proof-of-insurance information called RiskBlock. Ultimately, when this tool is fully deployed it will help law enforcement, insured and insurers verify insurance coverage in real time and accelerate claims processing.

Healthcare

- **MedicalChain**—The first healthcare company using blockchain technology to facilitate the storage and utilization of electronic health records in order to deliver a complete telemedicine experience. They are real practicing doctors in the UK healthcare structure and want to change the system from within.
- **MedRec**—In order to give any medical provider secure access [12].

1.10 Advantage and Disadvantage of Blockchain Technology

TABLE 2. Advantages and Disadvantages of blockchain technology [13]

S.NO.	ADVANTAGES	DISADVANTAGES
1	***Decentralization:*** This is the biggest advantage of Blockchain that it is not limited to a single central server. The technology made it possible to work on a decentralized server over a shared network. This is a primary feature which makes this technology different from the others. The database is not subjected to any of the single nodes instead it is distributed over all the nodes present on the shared network. In short, you don't have to pay a single penny to any third-party as there is no such thing involved.	***Signature Verification:*** A blockchain transaction requires a public-private cryptograph digital signature verification. It generally makes use of Elliptic Curve Digital Signature Algorithm (ECDSA). This algorithm makes sure that the transaction occurs between the right nodes. So, for every node to prove its authenticity, it needs to verify itself with a digital signature. This whole process is a bit tricky and complex one. While in a centralized database, there is no need for digital signature verification.
2	***Protection:*** Once a record has been stored in the ledger, it can only be deleted after a consensus. The transaction record gets the cryptographic protection. Thus, making this Blockchain technology a highly protected and secured one.	***Slow Performance:*** When this decentralized database is compared with a centralized database then you will get to know that it is much slower than the later one.

3	***Trust Factor:*** The technology makes sure that all the nodes get the complete ledger after every transaction. The transparency is the key to the trust developed by Blockchain. The shared ledger includes the details of the original source, destination, time, and date of the transactions.	***Consensus Approach:*** For a valid transaction to be added in the ledger, it needs the agreement of all the nodes. The process itself represents the extensive efforts of each node. Well, before establishing that a particular transaction is real and valid, all the nodes need to go through the various back and forth communications, which is again a lengthy process.
4	***Economically Feasible:*** As there is no third-party involvement, the cost is reduced automatically. Unlike other technologies, in Blockchain, the account holders can directly go for the peer-to-peer transaction by avoiding all the additional cost cutting.	***Redundant Data:*** The amount of computation required in Blockchain system is much more than in a centralized database. Every node running on this shared network needs to undergo the same process independently.
5	***Faster Transactions:*** Imagine a situation where you need to send money to a friend staying in another country. Generally, the process might take 3 – 10 working days. And in addition to that, you will be charged a few extra bucks for international money transfer. But, with the help of this technology, you can transfer the amount instantly and you will be subjected to a lesser charge for your transaction.	***Energy Consumption:*** For the validation process of each and every transaction, all the nodes present on the Blockchain network attempts 450 thousand trillion solutions in each passing second. This results in a significant amount of computer power consumption.

6	***Easy Sharing Database for Business to Business Arrangement:*** Different businesses rely on multiple computers for numerous databases. And it becomes difficult when one wants to share this database with another business. The simple solution is Blockchain technology as it maintains a single shared ledger. And it is easy to share this ledger with any other business.	
7	***All Time Accessibility:*** As this technology works on a decentralized network, so, even if any of the nodes break down, there will be no effect on the other nodes working on the same shared network. The ledger and the nodes will work as usual. In simple words, the complete system failure is near to impossible when Blockchain technology is considered. And thus, making the network accessible always.	

1.11 Background of Blockcerts

The concept of Blockcerts initiated by the MIT media lab. MIT media lab is a research laboratory at the Massachusetts Institute of Technology [19]. A team of researchers at MIT media lab gives the concept of Blockcerts during their research project led by Philipp Schmidt and Juliana Nazare along with many other professors. They collaborated with Learning Machine which is a software company at Cambridge to develop Blockcerts [20]. The need to introduce Blockcerts was to provide the student with a way of storing and verifying their credentials securely. Blockcerts also allow employers of the company to instantly validate the credentials of the student to prove their skills and proprietary.
Blockcerts can also be considered as metamorphic technology for those who have lost their credentials in some kind of disaster (can be a natural disaster, a situation of war). Due to these kinds of disasters, we have a situation of credentials missing, in that case, we are dependent on our universities which may don't exist or do not store our credentials for a longer time [21]. Hence, Blockcerts can help to get rid of these problems.

"I don't believe in one central body having ownership over the digital record of people's learning,"

- Philipp Schmidt [21].

Initially, the Blockcerts was taken as an experiment in which 619 MIT students can receive their diploma in digital form.Students were guided in such a way, to download Blockcerts Application and add MIT as an issuer.

"Before graduation, MIT sends the students an invite e-mail, which says 'Hey, go download the Blockcerts Wallet app, accept the pass phrase, and add MIT as an issuer,'"

-Chris Jagers [21].

After the course completion, MIT sends an email containing a digital certificate and ask the students to upload the certificate into Blockcerts application. Then the application sends that certificate to all the nodes in the blockchain. Moreover, blocks containing information about certificates created and verified by nodes. After that, the blocks are added to the existing blockchain, which can be accessed by the student using its private key [21] as explained in fig.5.

1.12 Working of Blockcerts and its Components

Blockcerts is an open infrastructure for the generation and validation of blockchain-based credentials. Blockcerts can be used to issue many kinds of certificates and identity documents in Government or Private sectors.

Components of Blockcerts

There are four components of Blockcerts which include Issuer, Certificate, Verifier and Blockcerts wallet application as discussed below [20]:

- **Issuer:** Issuer can be a university, governmental authority or any other organization that will issue or create a certificate by using recipient public key and digitally sign the certificate by using their private key.
- **Certificate:** Certificates are nothing but a digitally signed document that contains proof of an individual's skills and achievements.
- **Verifier:** Verifier can be anyone who will verify that the certificate has not tampered, issued by the particular authority and issued to a particular recipient
- **Wallet Application:** This is a platform where the recipient can securely store their certificate and can easily share it with anyone.

Working of Blockcerts

As we have discussed above the components of Blockcerts, all the components have their work in the process of certification. Let's take an overview of generating a birth certificate in which we have Government Authority (GA) as issuer, a recipient and a verifier as shown in fig.8.

ISSUING: GA will issue a digital certificate on blockchain for that, there will be the following steps:

- The GA will create a JSON file from the information provided to GA concerning certificate (which will contain recipient Name, DOB, name of the issuer, etc.).
- GA has its Blockchain address (pair of public /private key). The GA will digitally Sign the certificate using its own Private Key. So, the point of origin can be verified and will encrypt the JSON created using an encryption algorithm (SHA-256).

- Now, GA will invite the recipient to receive the blockchain credential. The recipient will accept the invitation and will share its blockchain address.
- Then the GA will perform a blockchain transaction from their address to recipient address by using the recipient's public key and send the blockchain credentials to the recipient.
- The recipient will use its private key to decrypt the JSON file to read it.

VERIFYING: Here comes another component of Blockcerts which is verifier. The blockchain certificates are sharable as shown in fig-9. Let suppose the recipient shares the certificate along with transaction details to the third person, then that third person will play the role of the verifier. Now, the verifier will be able to verify the certificate provided by the recipient that the certificate present on the blockchain is the same or not. The verification can be done by uploading a JSON certificate on Blockcerts application

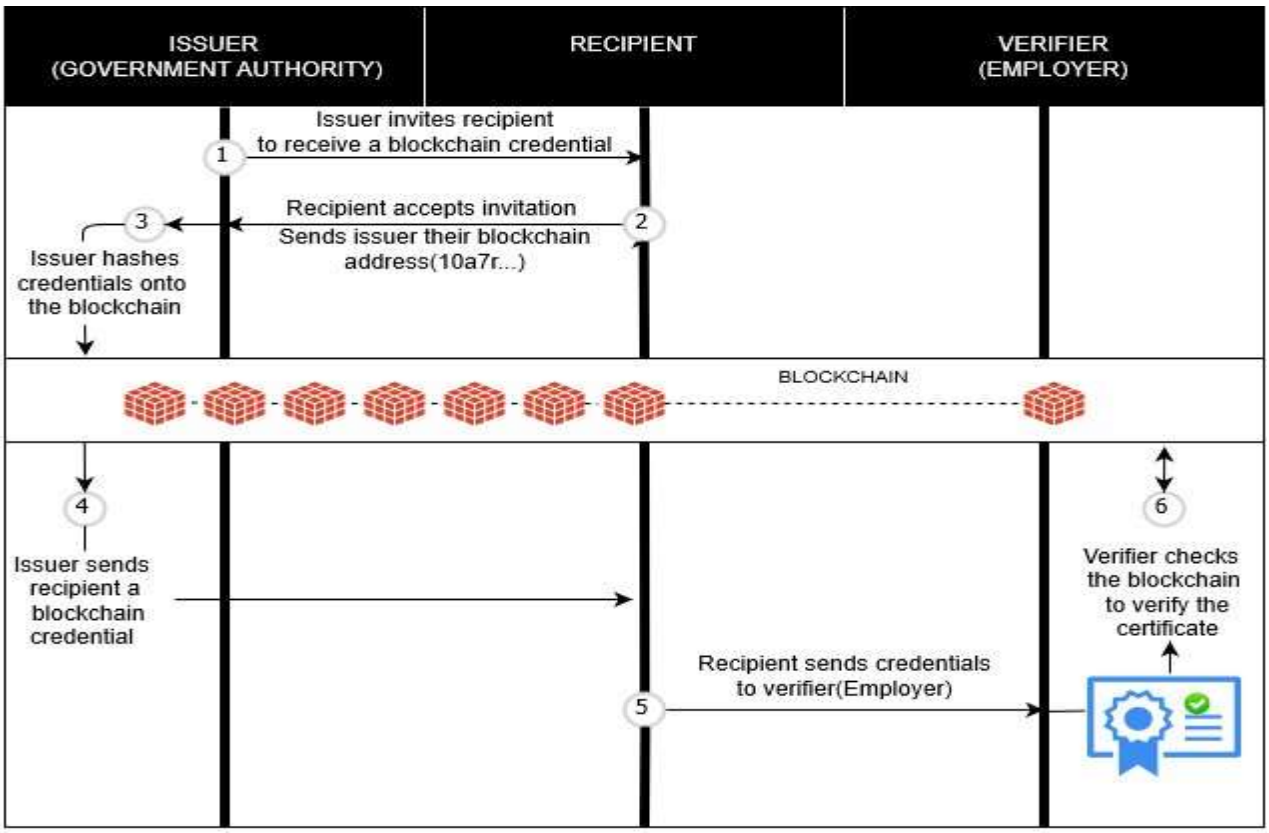


Figure 9: Working of Blockcerts

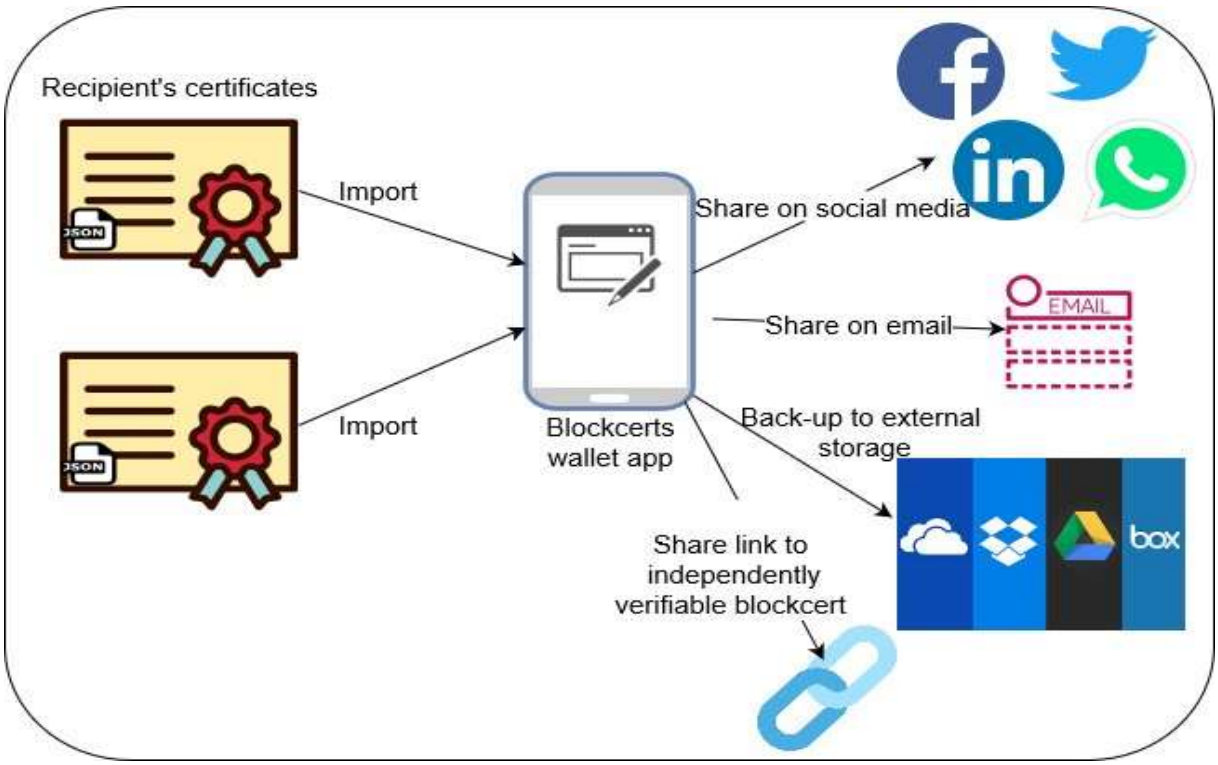


Figure 10: Shareability of Blockchain-based certificate.

1.13 Certification Process using Blockchain Technology and Blockcerts Application

In figure 10, the working of blockchain is explained for the certification process. There are mainly six steps in the overall process of certification. In the first step, the user will provide the details and legit documents that are generally required in the process of birth/death certification respectively. In the second step, a block will be created which contains relevant information regarding the certificate. Now, this block will be broadcasted to every node in the blockchain. Then, in the fourth step, all the nodes will validate the details provided by the user in the first step. After validation new block is added to the existing verified blockchain. At last, the certification process is completed by using Blockcerts.

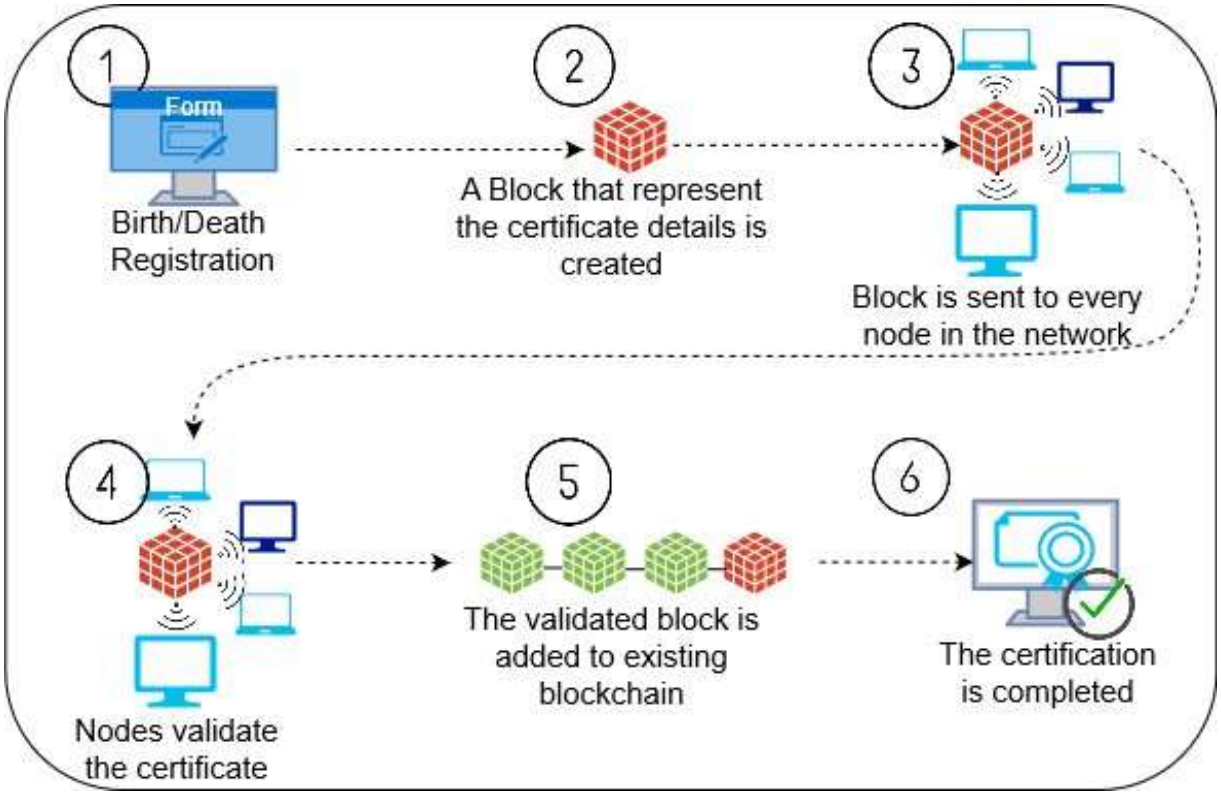


Figure 7: Certification Process using Blockchain Technology and Blockcerts Application

CHAPTER 2

LITERATURE SURVEY

First, a common ground by searching generally for the concepts across various platforms to identify a knowledge base as the foundation for the literature review was stablished. As established above, the primary focus has been on the keyword “blockchain” “technology” and “distributed ledger”, due to the fact that extensive literature exists on “platforms”. Second, when the common ground has been established, we identify the primary drivers within the OI research field (Chesbrough and Bogers, 2014) (Bogers et al., 2017). We take foundation in the senior scholar’s basket of journals, in which we identify the basket of eight, consisting of the essential journals within OI research. However, we note that due to the exclusion of technical papers, we cannot claim to be exhaustive, being it such an emerging research area. During our general search, we start out by searching for literature on Google Scholar to create a quick overview of the research topic and reach many valuable social media publications. 4 However, as the topic is considered so novel, we also checked the main conference publications within OI to ensure that the topic has been exhaustively examined

2.2 Related Work

With the advancement in the field of Blockchain Technology, researchers have proposed many survey papers based on the advantages of this technology in several fields like Privacy & Identity, Security Services, Verification, Tampering and other survey-based on Blockchain include Healthcare, Cryptocurrency, etc.

- **Conceptual Blockchain Based Survey**

  Tara Salman, Maede Zolanvari and Aiman Erbad [4] present various security services like confidentiality, integrity, availability, and authentication. In their survey, they explain how the Blockchain-based system is more preferable to a traditional centralized system in the context of services. Shixiong Yao, Jing Chen, and Kun He [6] define how to preserve the privacy using the Blockchain approach in which they explain to store the necessary information (name, hash value, and other related operation) in blockchain and it utilizes another secondary storage for detailed information about certificates. And also, to deal with an unclear query regarding certificate status, thus preserving the privacy.

  Nitin Kumavat, Swapnil Mengade, Dishant Desai [3] describes to tackle the problem of fake certificate and verify the authenticity of certificates. In their survey, they describe the manual process of verifying the certificate. And they are solving this problem by storing digital certificates in Blockchain which makes the verification task easier and there are fewer chances of producing a fake certificate.

  Maharshi Shah, Priyanka Kumar [7] gives the theoretical concept about an unmodifiable digital birth certificate. In their survey, they use PKI (public key infrastructure) to validate the integrity of the certificate.

- **Differentiating our research work from related work**

  This paper describes the model in which we are using the concept of Blockcerts to build the application which will generate the Birth/Death certificate based on the information stored in the blockchain. Furthermore, the verification of the certificate will be done by using the concept of public/private key cryptography. The generated certificate will be stored in the blockchain as a new transaction. The stored certificate can be easily validated and retrieved whenever required. This is how we will remove the problem of a fake and missing certificate.

CHAPTER 3

PROBLEM DESCRIPTION AND PROPOSED WORK

3.1 Problem Description

As we know that Birth/Death Certificates are very essential documents. Birth Certificate can be used as proof of an individual's age, for academics, for jobs and can be used as an identity for various government documents (Passport, Driving License, Voter-ID, etc.). Likewise, Death Certificates can be used by the family of deceased to inherit property, to claim insurance benefits and used by the government to maintain population statistics. In the current scenario, due to the complex procedure of applying and getting a certificate, nearly half of the world's population does not have a birth certificate. Also, authentication of a valid certificate is a laborious task. At the same time, due to the presence of hard copy, missing certificate becomes a crucial problem and re-issuing of that certificate is a hectic process. Presently, the digital certificate is a way to tackle the problem of missing certificates still it is not sufficient as it can tamper easily.

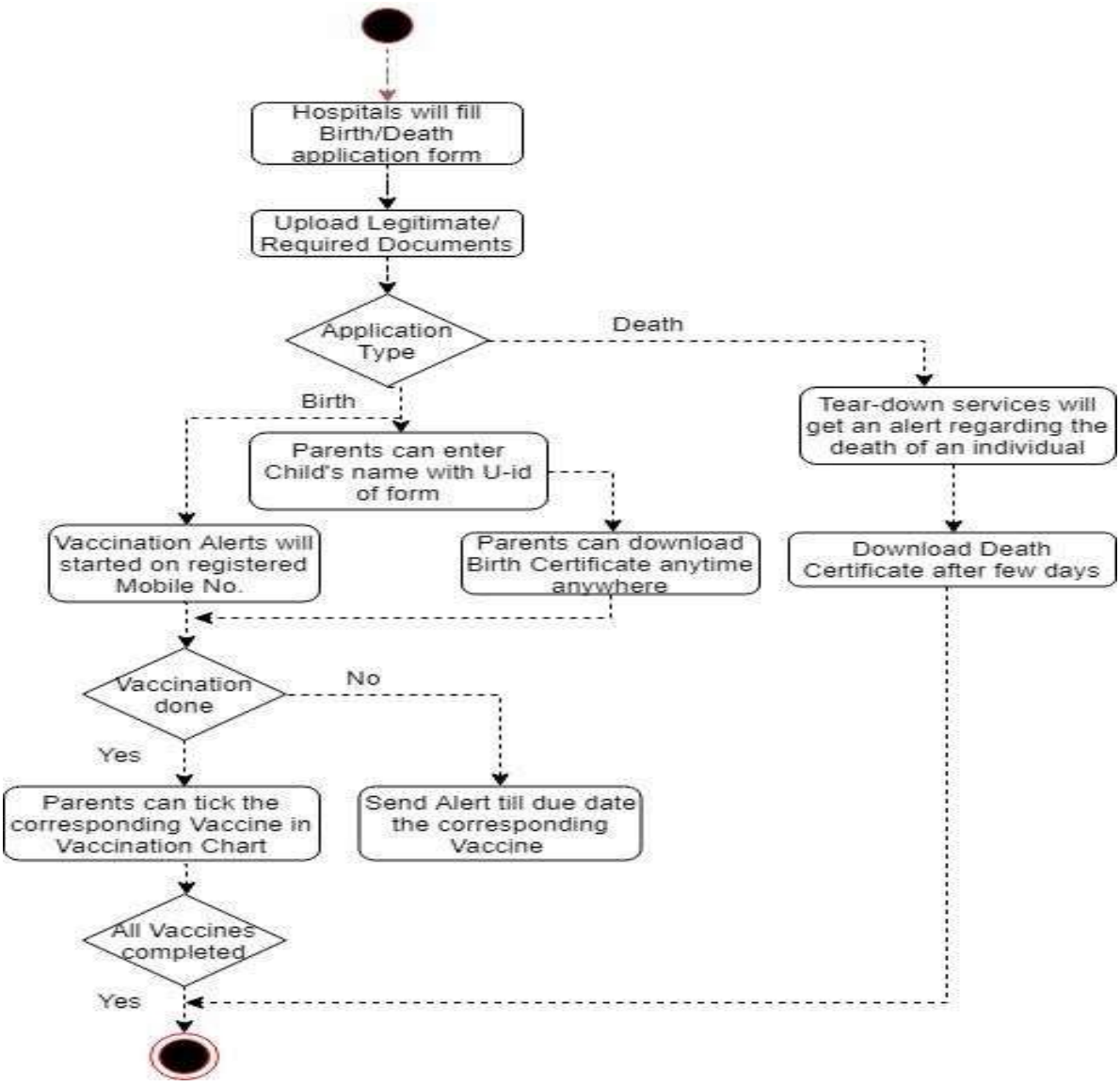
3.2 Proposed Work

The objective of this model is to give the solution to issue Birth/Death certificates and validation of certificates using Blockcerts which is based on Blockchain Technology. Blockcerts is used for issuing and verifying a blockchain-based formal transaction. Blockchain is a shared distributed, decentralized database system used to store information and this information cannot tamper easily. It also provides security services like confidentiality, authentication, integrity. Here, we have developed a blockchain based mobile application and web application as a solution of this problem statement.

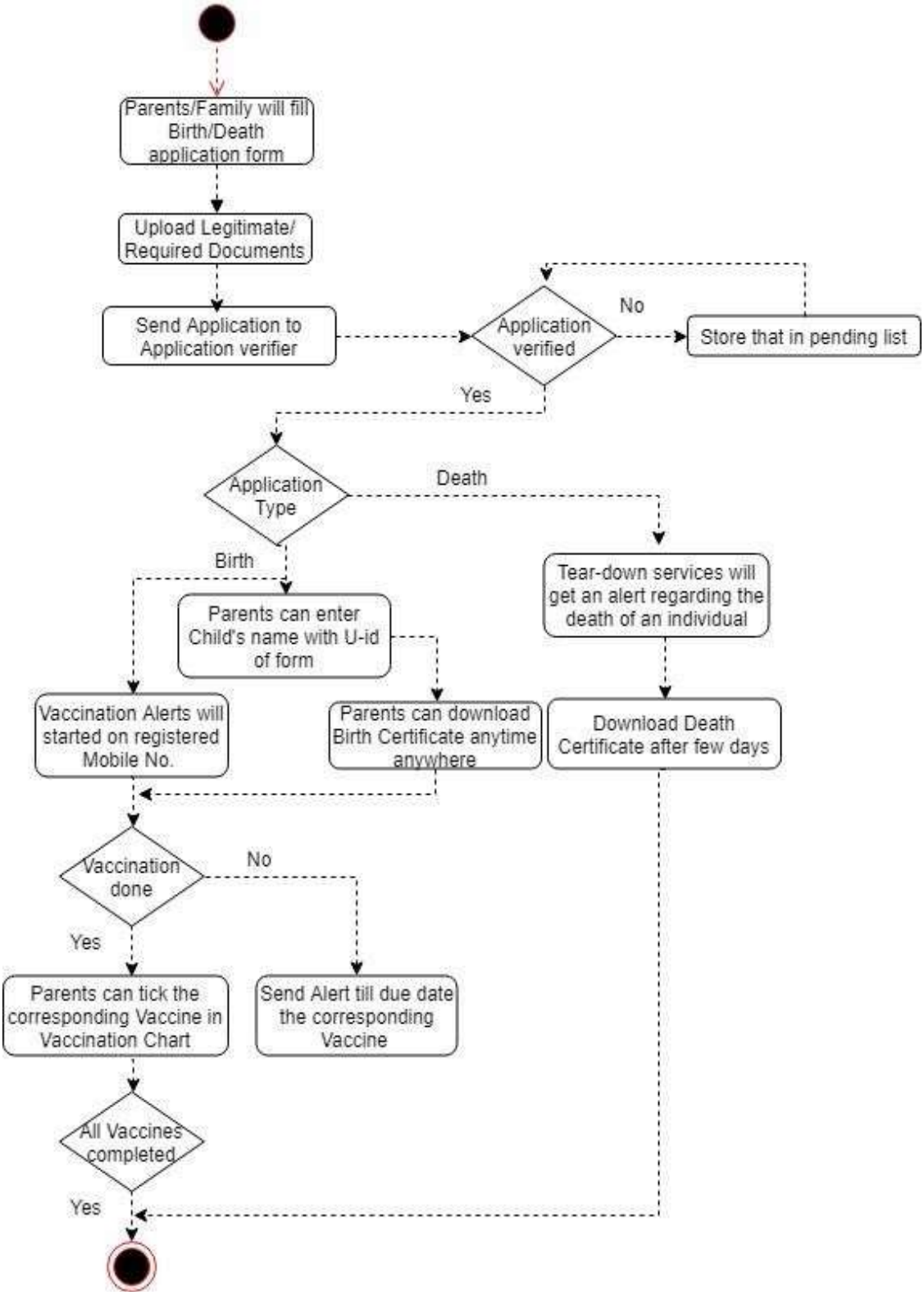
CHAPTER 4

IMPLEMENTATION AND RESULT DISCUSSION

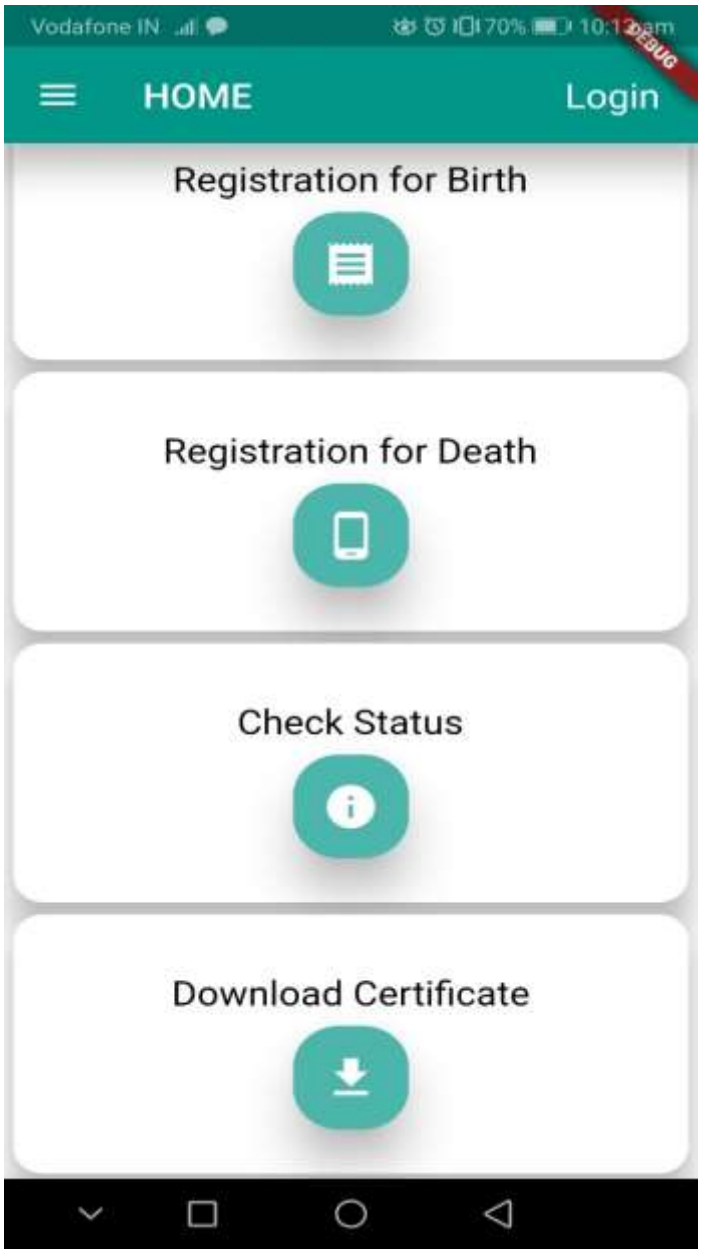
4.1 Use Case Diagram for Hospital Module

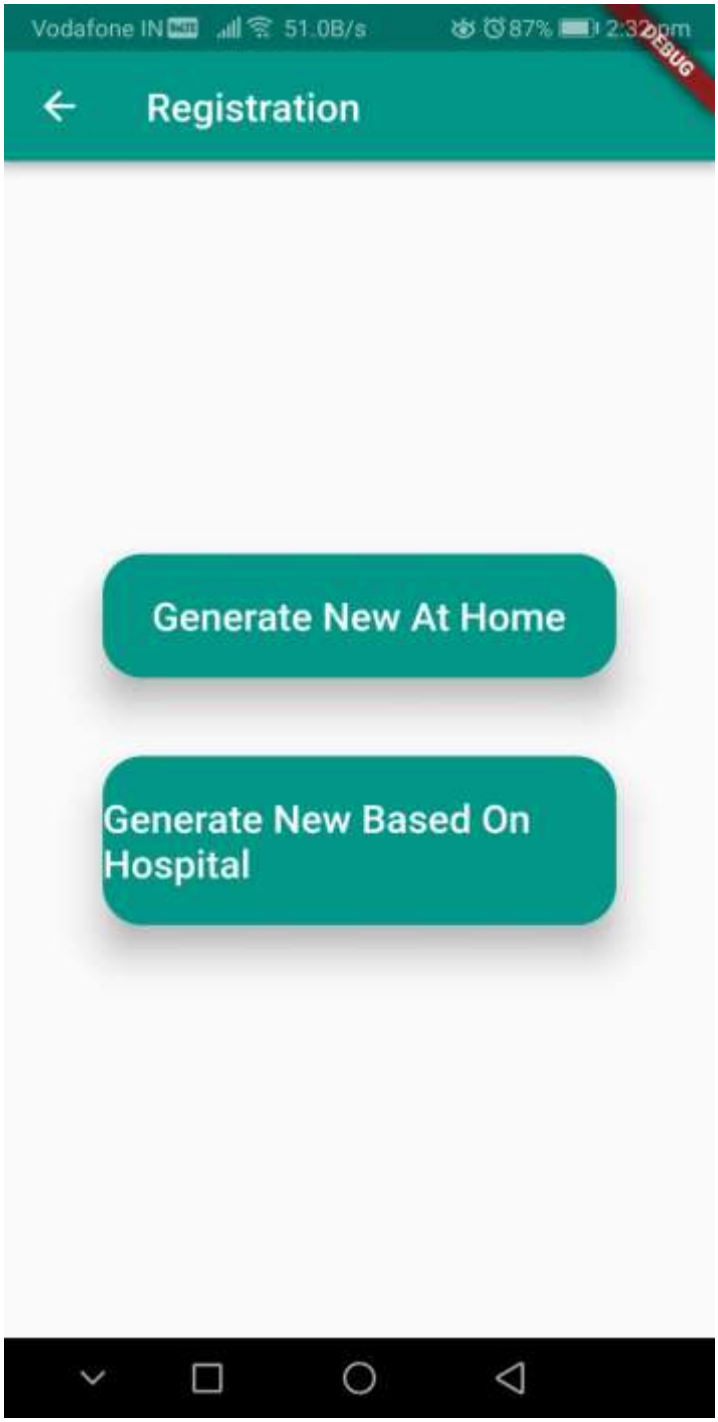


4.2 Use Case Diagram for Home Module



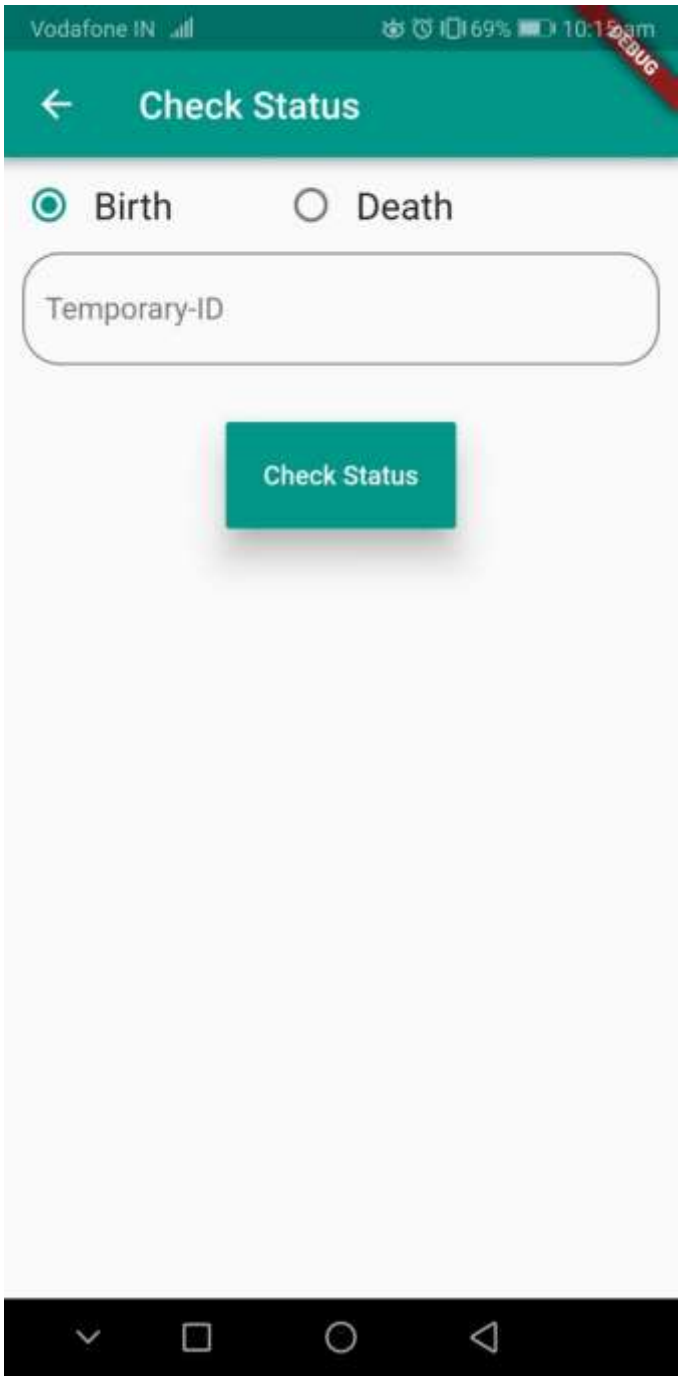
4.3 Flow of Application (Mobile App) Screenshots

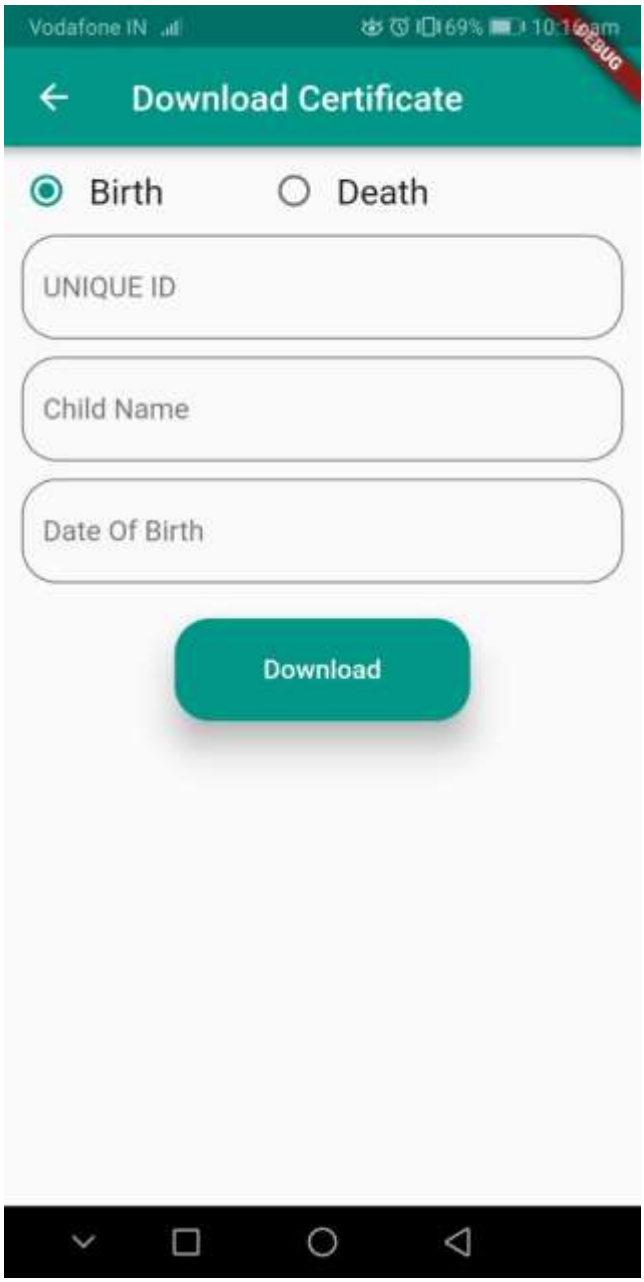


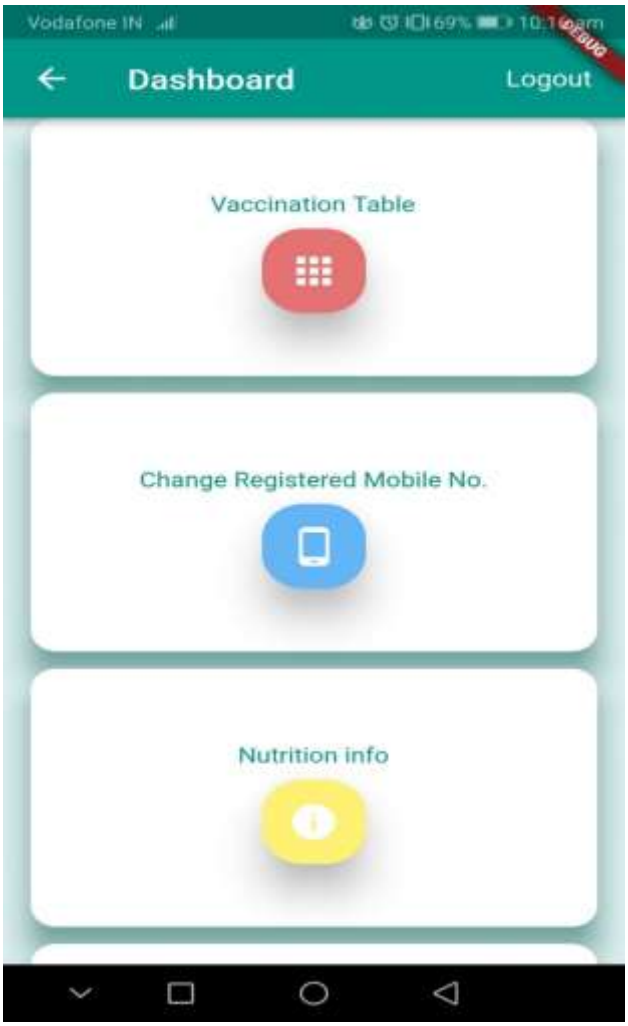

Vodafone IN
51.0B/s
87%
2:32 pm
DEBUG
Registration
Generate New At Home
Generate New Based On Hospital

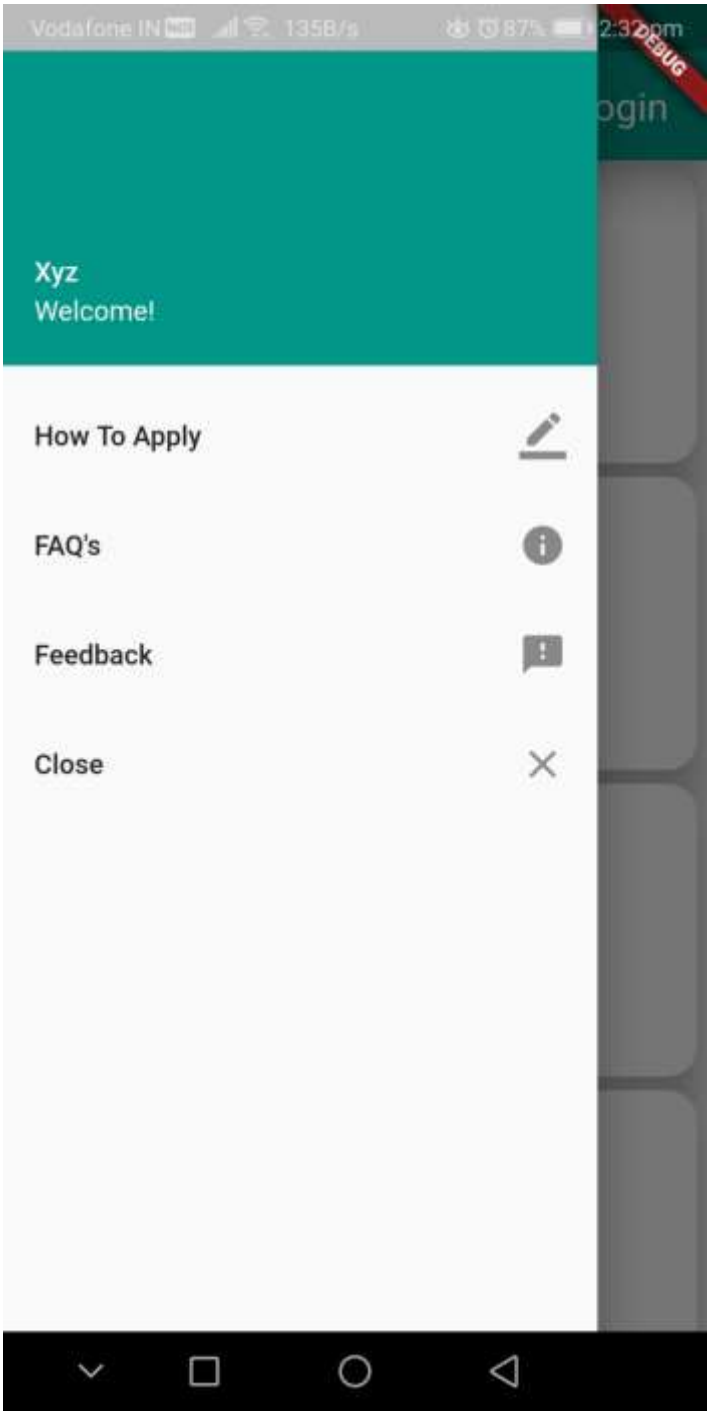

Vodafone IN
70%
10:1
DEBUG
Registration Form
LEGAL INFORMATION
Information of the Child
Date of Birth
dd/mm/yyyy
Time Of Birth
Sex
First Name
Middle Name
Last Name
Place of birth
State

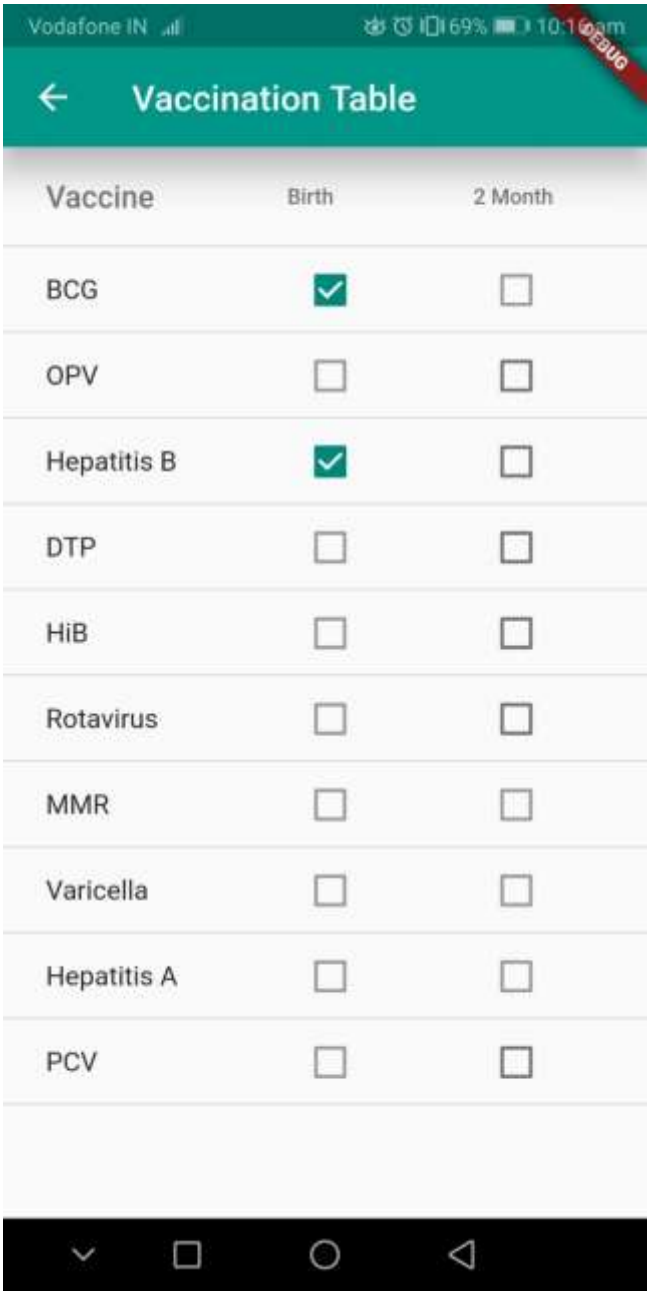

Vodafone IN
45.7B/s
68%
DEBUG
Registered
Thank You for Registration Your Temporary Id is "XYZ"

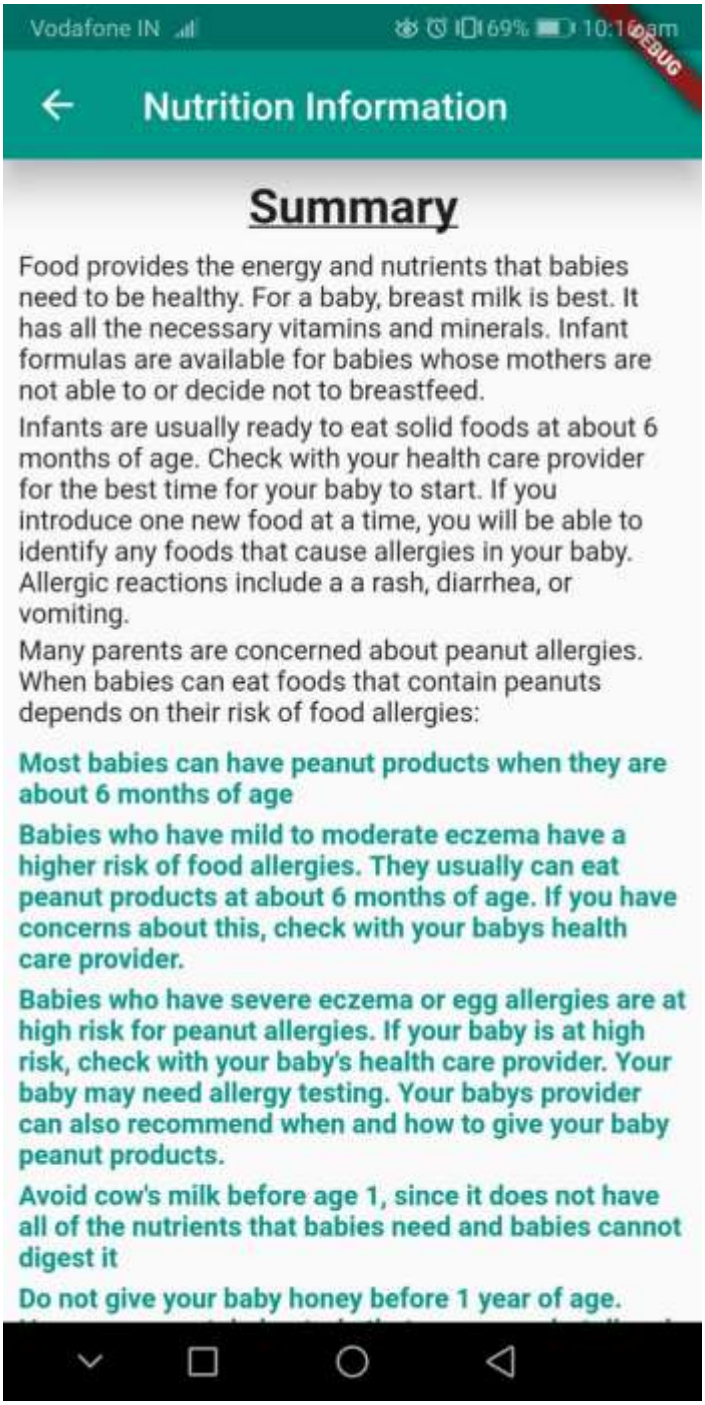

Vodafone IN
69%
DEBUG
Check Status
Birth
Death
Temporary-ID
Check Status

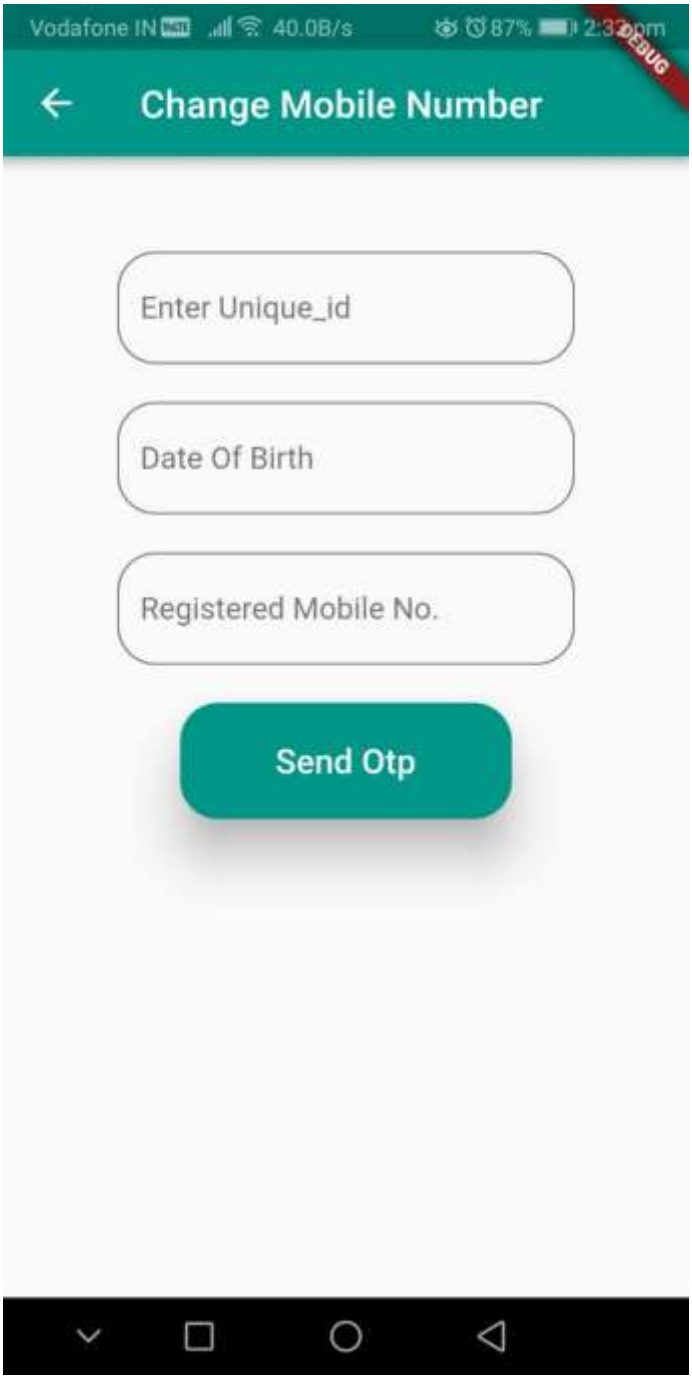

Vodafone IN
69%
DEBUG
Download Certificate
Birth
Death
UNIQUE ID
Child Name
Date Of Birth
Download

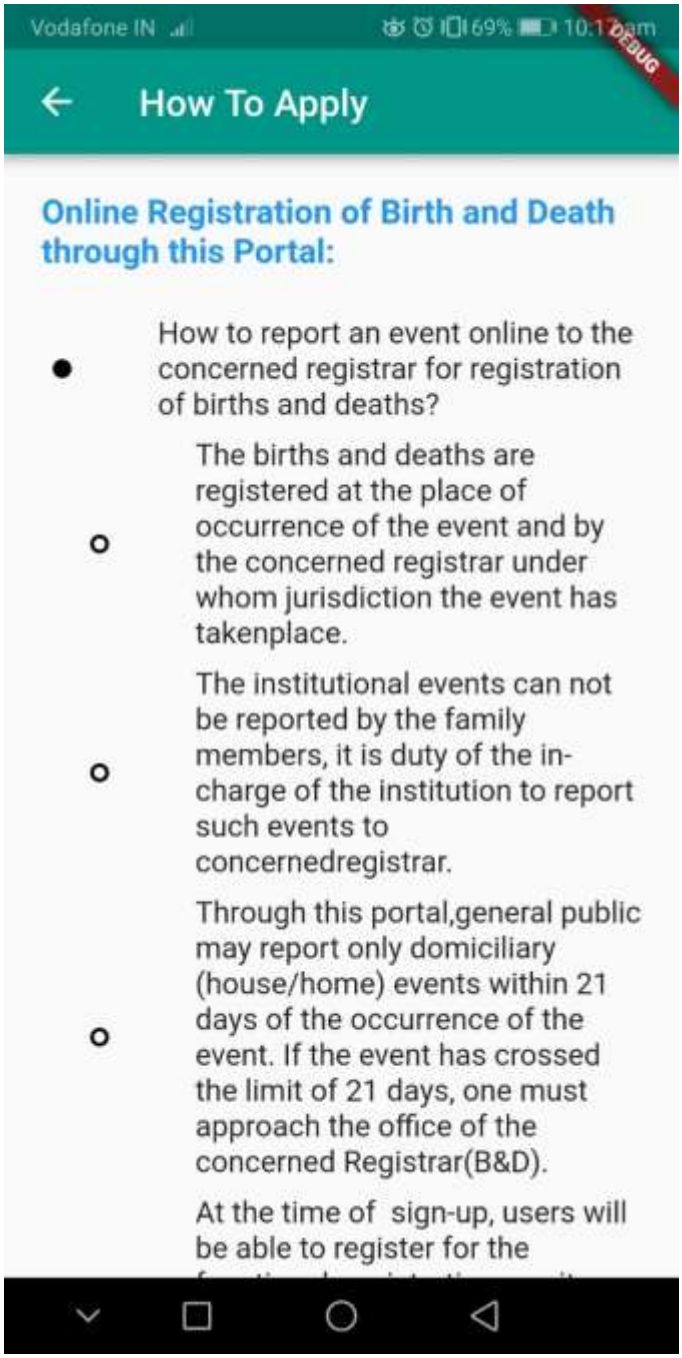

Vodafone IN
69%
10:1 am
DEBUG
Dashboard
Logout
Vaccination Table
Change Registered Mobile No.
Nutrition info


Vodafone IN
135B/s
87%
2:32 pm
DEBUG
ogin
Xyz
Welcome!
How To Apply
FAQ's
Feedback
Close

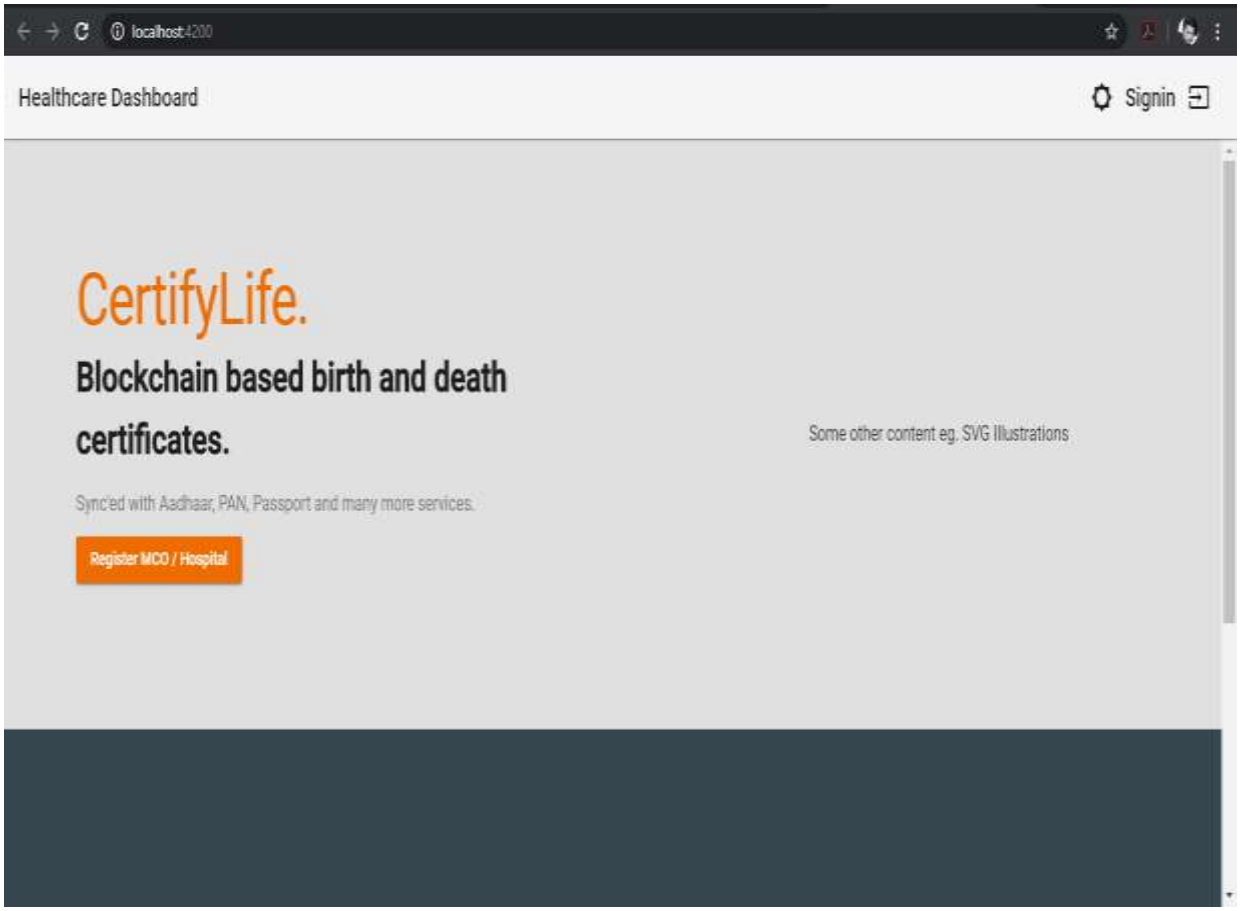

Vodafone IN
69%
DEBUG
Vaccination Table
Vaccine
Birth
2 Month
BCG
OPV
Hepatitis B
DTP
HiB
Rotavirus
MMR
Varicella
Hepatitis A
PCV

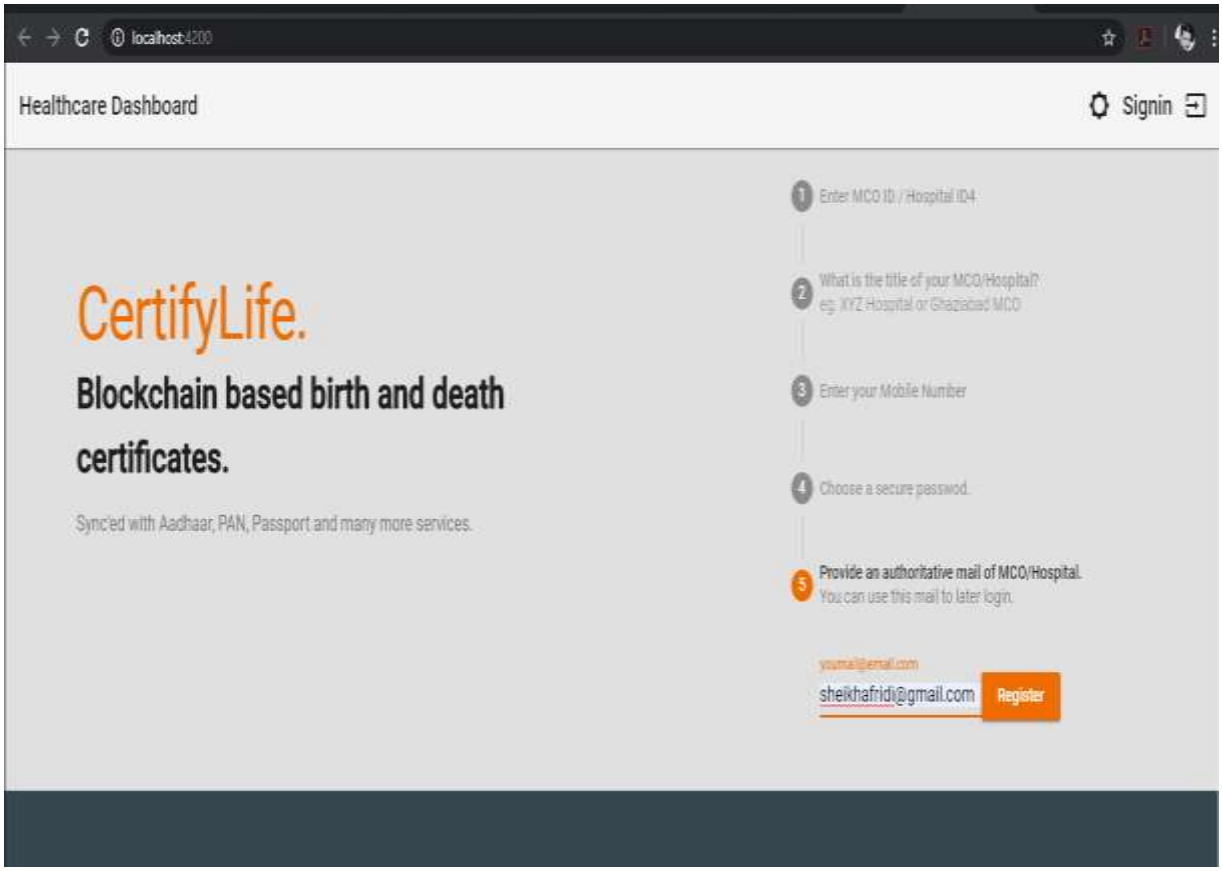

Vodafone IN
69%
DEBUG
Nutrition Information
Summary
Food provides the energy and nutrients that babies need to be healthy. For a baby, breast milk is best. It has all the necessary vitamins and minerals. Infant formulas are available for babies whose mothers are not able to or decide not to breastfeed.
Infants are usually ready to eat solid foods at about 6 months of age. Check with your health care provider for the best time for your baby to start. If you introduce one new food at a time, you will be able to identify any foods that cause allergies in your baby. Allergic reactions include a a rash, diarrhea, or vomiting.
Many parents are concerned about peanut allergies. When babies can eat foods that contain peanuts depends on their risk of food allergies:
Most babies can have peanut products when they are about 6 months of age
Babies who have mild to moderate eczema have a higher risk of food allergies. They usually can eat peanut products at about 6 months of age. If you have concerns about this, check with your babys health care provider.
Babies who have severe eczema or egg allergies are at high risk for peanut allergies. If your baby is at high risk, check with your baby's health care provider. Your baby may need allergy testing. Your babys provider can also recommend when and how to give your baby peanut products.
Avoid cow's milk before age 1, since it does not have all of the nutrients that babies need and babies cannot digest it
Do not give your baby honey before 1 year of age.

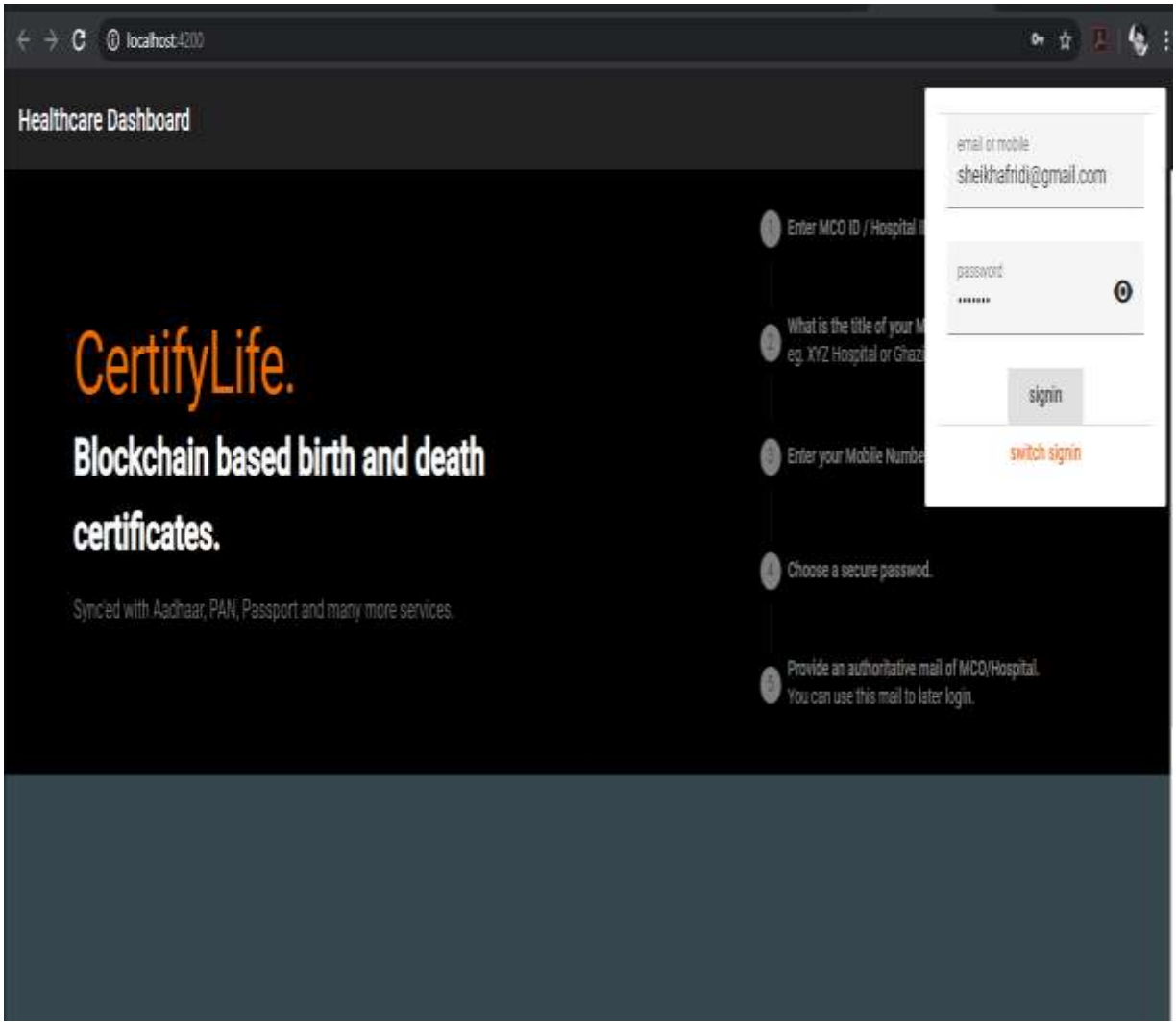

Vodafone IN
40.0B/s
87%
DEBUG
Change Mobile Number
Enter Unique_id
Date Of Birth
Registered Mobile No.
Send Otp

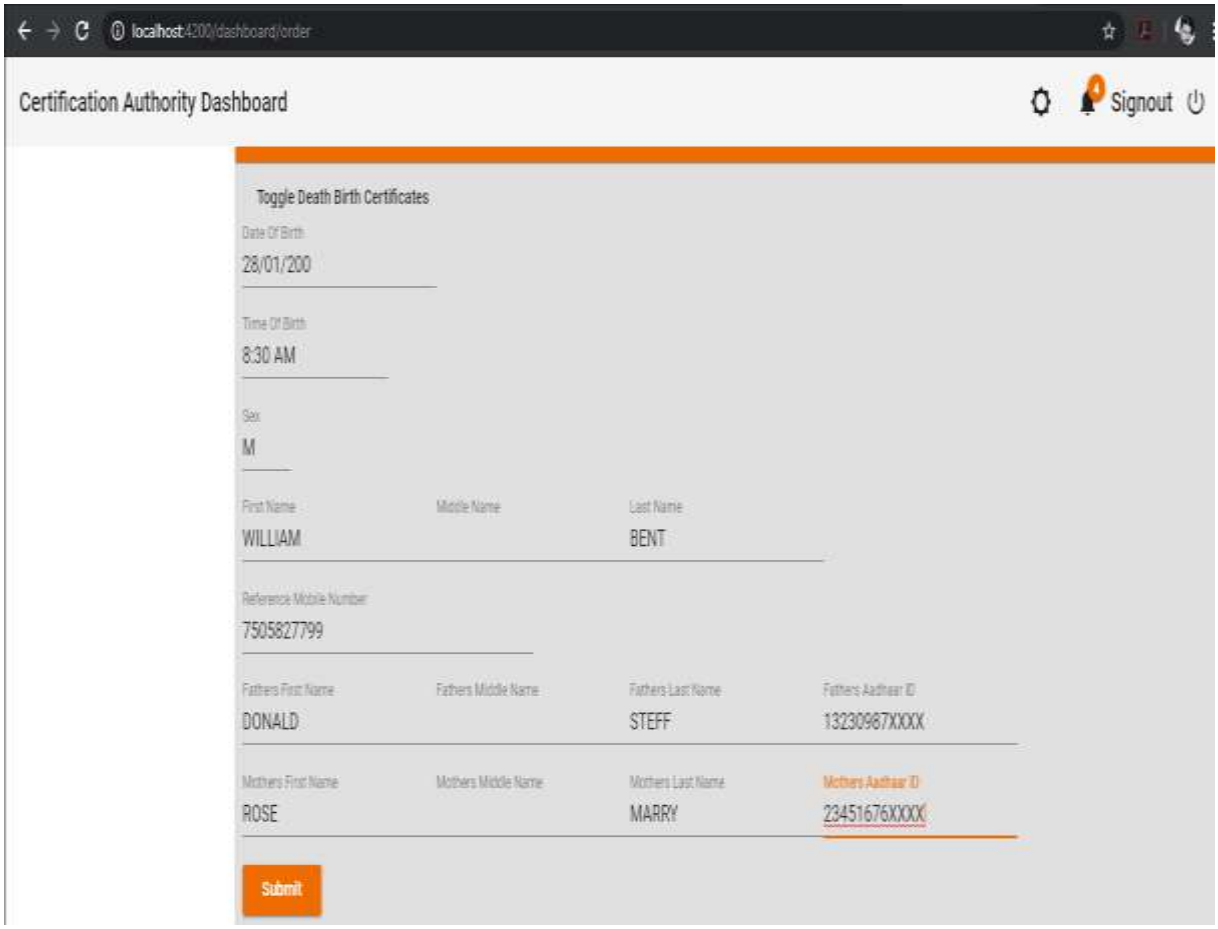

Vodafone IN
69%
DEBUG
How To Apply
Online Registration of Birth and Death through this Portal:
How to report an event online to the concerned registrar for registration of births and deaths?
The births and deaths are registered at the place of occurrence of the event and by the concerned registrar under whom jurisdiction the event has takenplace.
The institutional events can not be reported by the family members, it is duty of the in-charge of the institution to report such events to concernedregistrar.
Through this portal,general public may report only domiciliary (house/home) events within 21 days of the occurrence of the event. If the event has crossed the limit of 21 days, one must approach the office of the concerned Registrar(B&D).
At the time of sign-up, users will be able to register for the

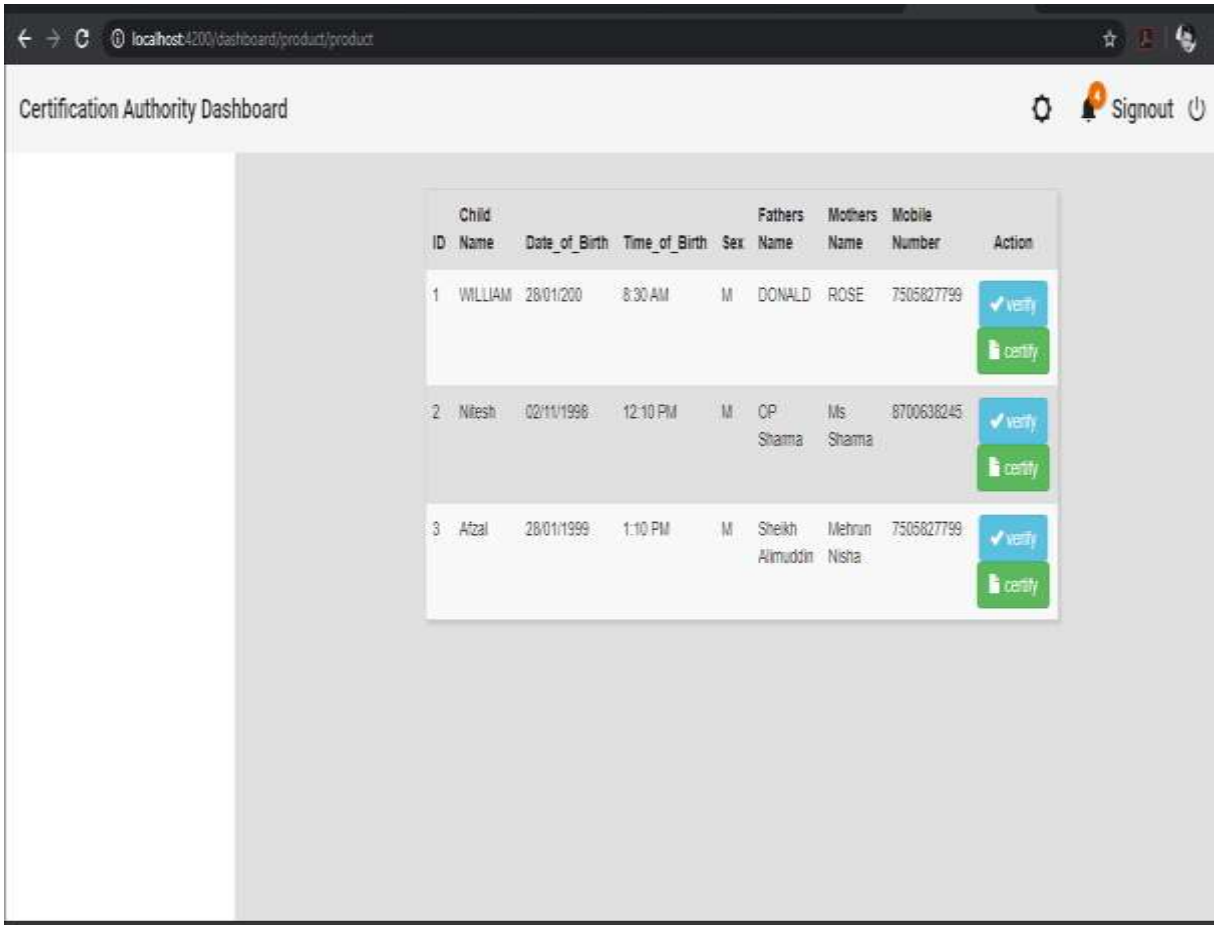
4.4 Flow of Application (Web Portal) Screenshot

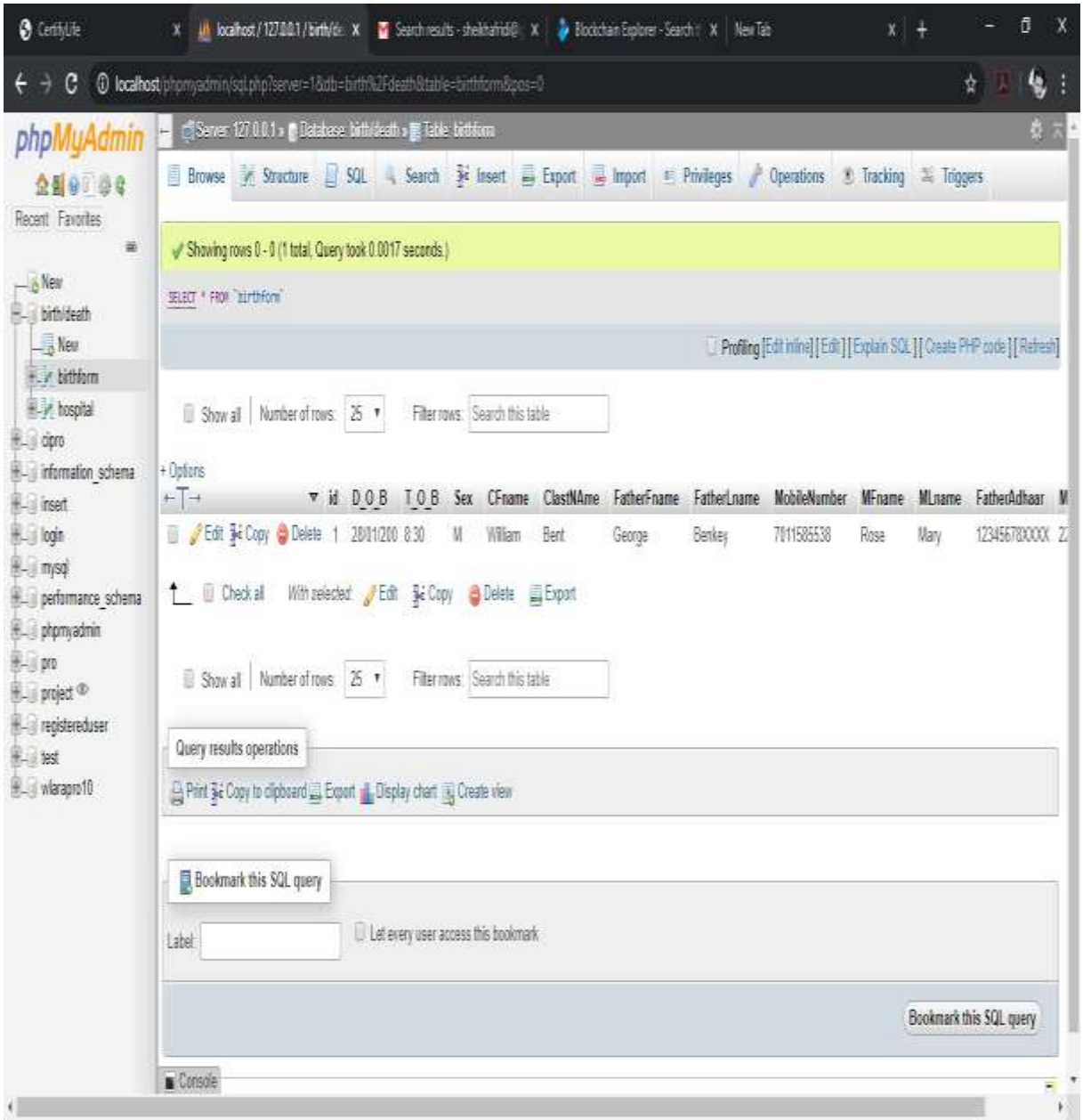


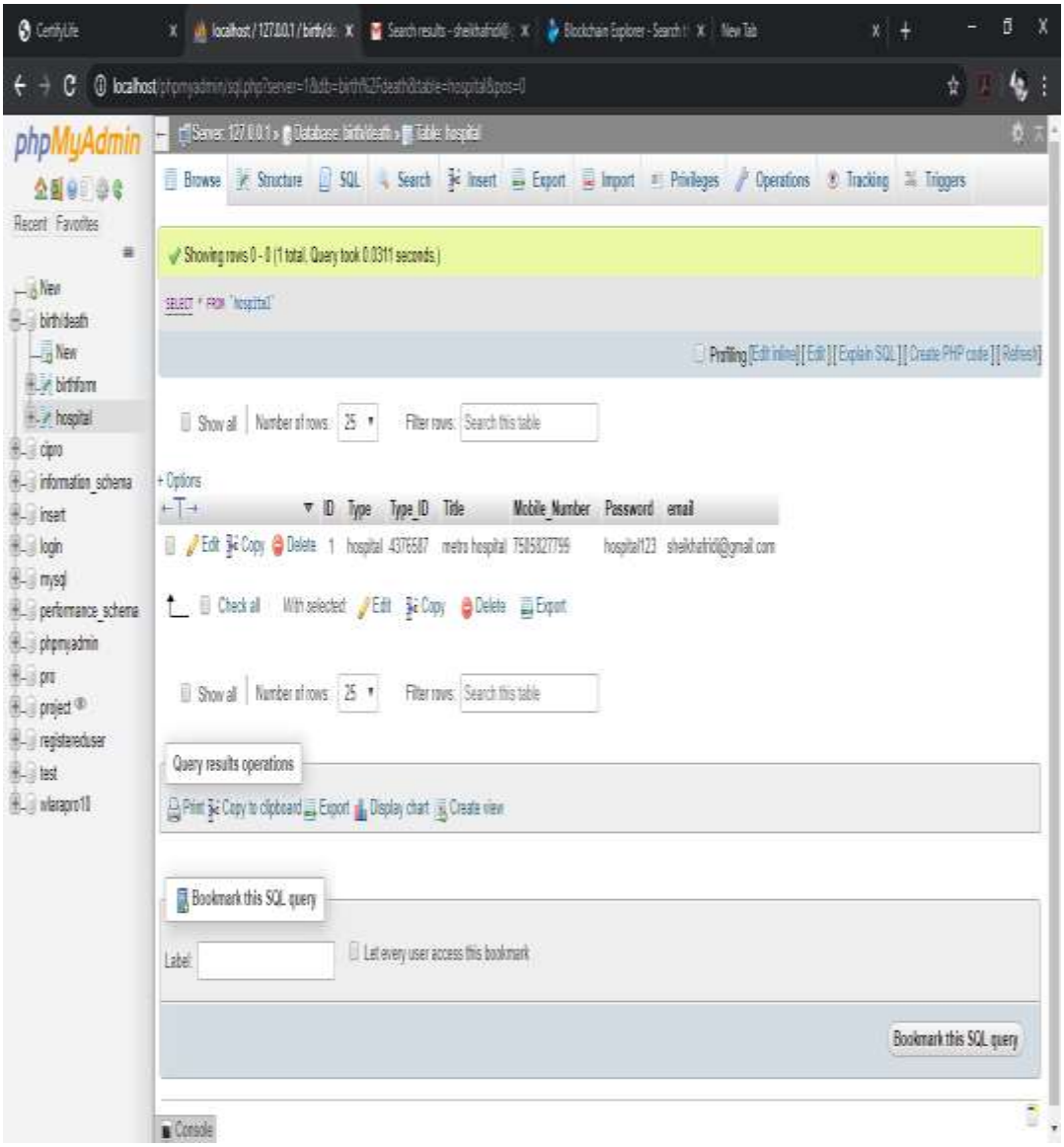

localhost:4200
Healthcare Dashboard
Signin
CertifyLife.
Blockchain based birth and death certificates.
Sync'ed with Aadhaar, PAN, Passport and many more services.
1 Enter MCO ID / Hospital ID4
2 What is the title of your MCO/Hospital?
eg. XYZ Hospital or Ghaziabad MCO
3 Enter your Mobile Number
4 Choose a secure passwod.
5 Provide an authoritative mail of MCO/Hospital.
You can use this mail to later login.
sheikhafridi@gmail.com
Register


localhost:4200
Healthcare Dashboard
email or mobile
sheikhafridi@gmail.com
password
signin
switch signin
CertifyLife.
Blockchain based birth and death certificates.
Synced with Aadhaar, PAN, Passport and many more services.
Enter MCO ID / Hospital
What is the title of your
eg. XYZ Hospital or Ghaz
Enter your Mobile Numbe
Choose a secure passwod.
Provide an authoritative mail of MCO/Hospital.
You can use this mail to later login.

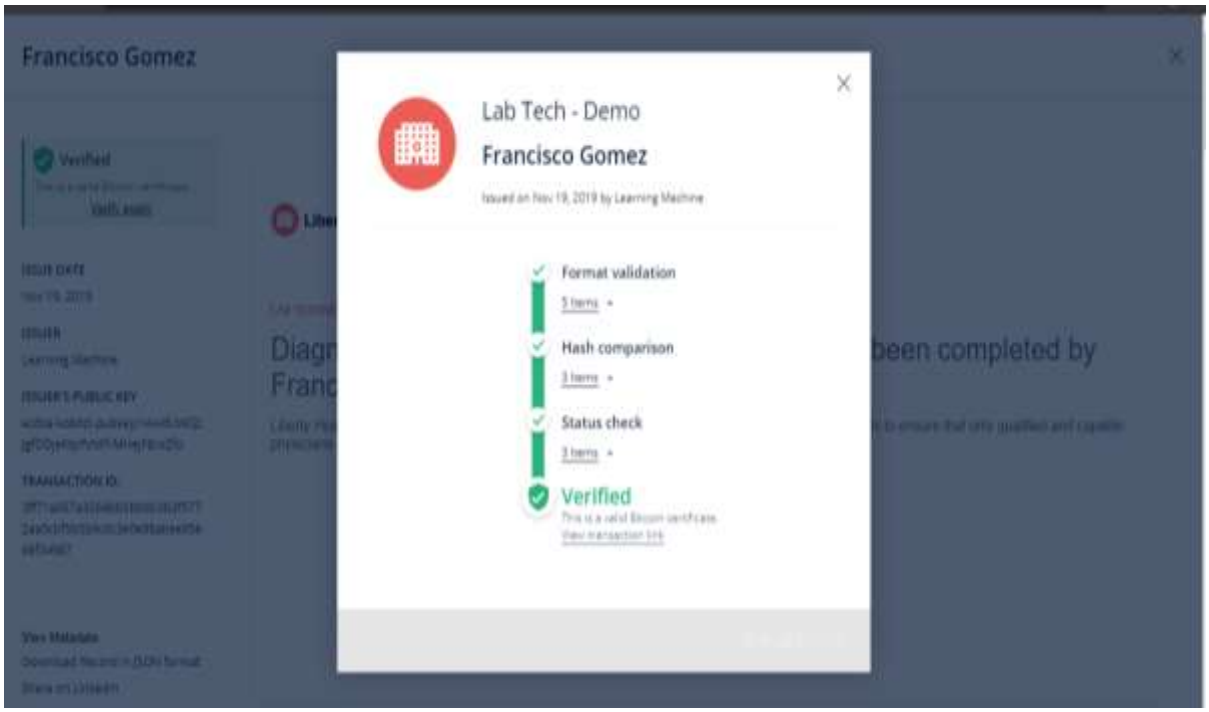

localhost:4200/dashboard/order
Certification Authority Dashboard
Signout
Toggle Death Birth Certificates
Date Of Birth
28/01/200
Time Of Birth
8:30 AM
Sex
M
First Name
Middle Name
Last Name
WILLIAM
BENT
Reference Mobile Number
7505827799
Fathers First Name
Fathers Middle Name
Fathers Last Name
Fathers Aadhaar ID
DONALD
STEFF
13230967XXXX
Mothers First Name
Mothers Middle Name
Mothers Last Name
Mothers Aadhaar ID
ROSE
MARRY
23451676XXXX
Submit

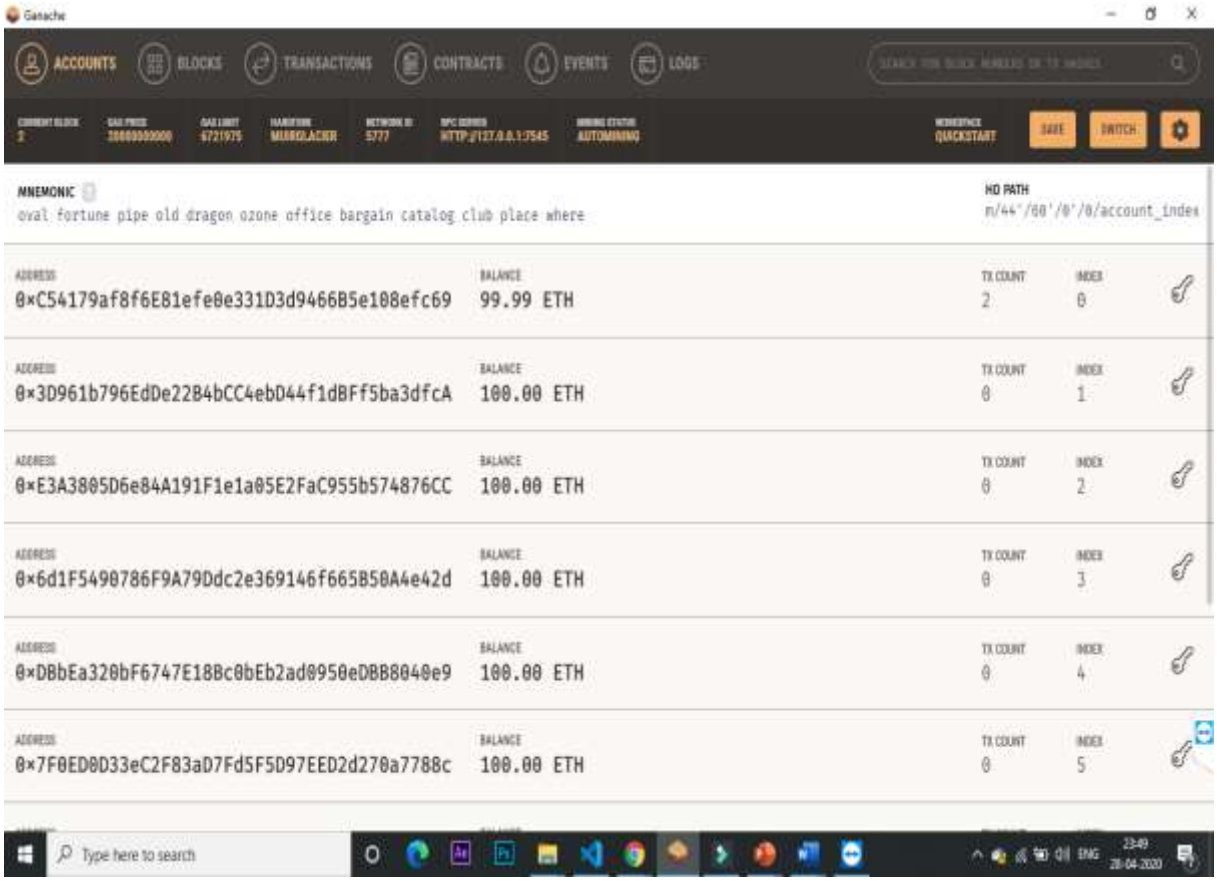

localhost:4200/dashboard/product/product
Certification Authority Dashboard
Signout
ID
Child Name
Date_of_Birth
Time_of_Birth
Sex
Fathers Name
Mothers Name
Mobile Number
Action
1
WILLIAM
28/01/200
8:30 AM
M
DONALD
ROSE
7505827799
verify
certify
2
Nitesh
02/11/1996
12:10 PM
M
OP Sharma
Ms Sharma
8700638245
verify
certify
3
Afzal
28/01/1999
1:10 PM
M
Sheikh Alimuddin
Mehrun Nisha
7505827799
verify
certify

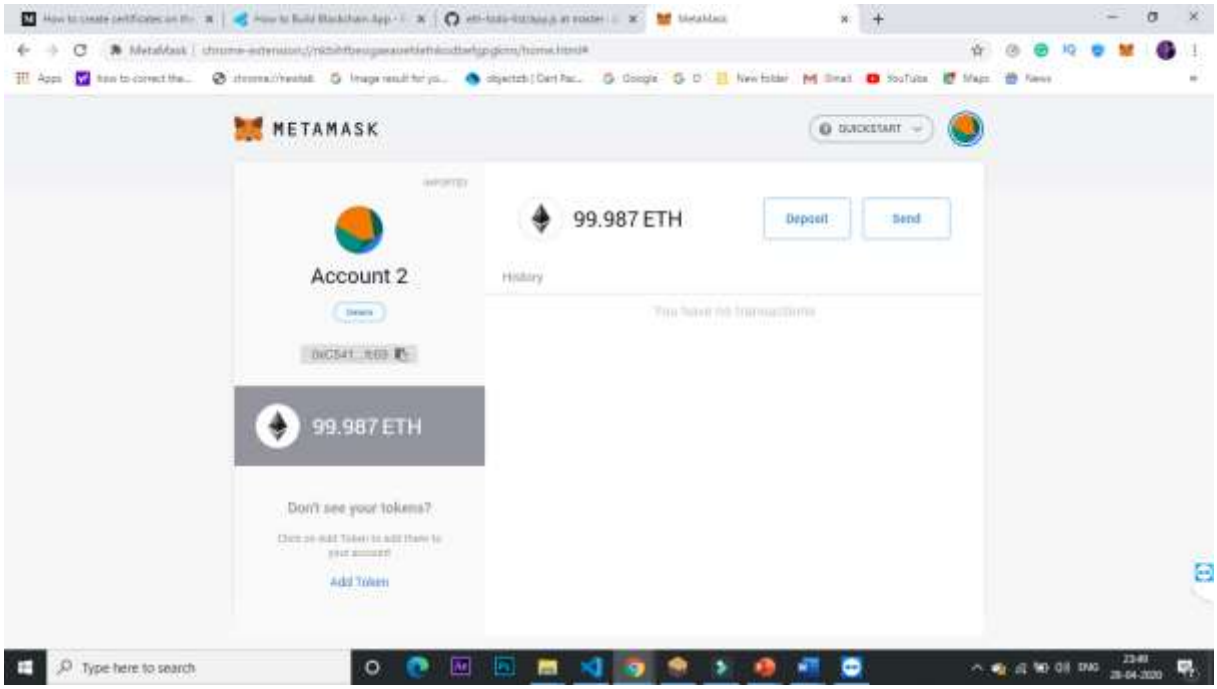

phpMyAdmin
Recent Favorites
New
birth/death
New
birthform
hospital
cipro
information_schema
insert
login
mysql
performance_schema
phpmyadmin
pro
project
registereduser
test
wlerapro10
Server: 127.0.0.1 » Database: birth/death » Table: birthform
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking
Triggers
Showing rows 0 - 0 (1 total, Query took 0.0017 seconds.)
SELECT * FROM `birthform`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
+ Options
id
D_O_B
T_O_B
Sex
CFname
ClastNAme
FatherFname
FatherLname
MobileNumber
MFname
MLname
FatherAdhaar
Edit
Copy
Delete
1
28/01/200
8:30
M
William
Bent
George
Benkey
7011585538
Rose
Mary
123456780XXX
Check all
With selected:
Edit
Copy
Delete
Export
Show all
Number of rows: 25
Filter rows: Search this table
Query results operations
Print
Copy to clipboard
Export
Display chart
Create view
Bookmark this SQL query
Label:
Let every user access this bookmark
Bookmark this SQL query
Console


phpMyAdmin
Recent Favorites
New
birthdeath
New
birthform
hospital
cipro
information_schema
insert
login
mysql
performance_schema
phpmyadmin
pro
project
registereduser
test
wiraapro10
Server: 127.0.0.1 » Database: birthdeath » Table: hospital
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking
Triggers
Showing rows 0 - 0 (1 total, Query took 0.0311 seconds.)
SELECT * FROM `hospital`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
+ Options
ID Type Type_ID Title Mobile_Number Password email
Edit Copy Delete 1 hospital 4376587 metro hospital 7585827799 hospital123 shaikhafrid@gmail.com
Check all
With selected:
Edit
Copy
Delete
Export
Show all
Number of rows: 25
Filter rows: Search this table
Query results operations
Print
Copy to clipboard
Export
Display chart
Create view
Bookmark this SQL query
Label:
Let every user access this bookmark
Bookmark this SQL query
Console


blockcerts.org
BLOCKCERTS
HOME
GUIDE
ABOUT
COMMUNITY
GITHUB
GET THE APP
Blockcerts Universal Verifier
Verify
Choose JSON file (you can also drag & drop your file)


Francisco Gomez
Lab Tech - Demo
Francisco Gomez
Format validation
Hash comparison
Status check
Verified


Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
MNEMONIC
oval fortune pipe old dragon ozone office bargain catalog club place where
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS
0x C54179af8f6E81efe0e331D3d9466B5e108efc69
BALANCE
99.99 ETH
TX COUNT
2
INDEX
0
ADDRESS
0x 3D961b796EdDe22B4bCC4ebD44f1dBFf5ba3dfcA
BALANCE
100.00 ETH
TX COUNT
0
INDEX
1
ADDRESS
0x E3A3805D6e84A191F1e1a05E2FaC955b574876CC
BALANCE
100.00 ETH
TX COUNT
0
INDEX
2
ADDRESS
0x 6d1F5490786F9A79Ddc2e369146f665B50A4e42d
BALANCE
100.00 ETH
TX COUNT
0
INDEX
3
ADDRESS
0x DBbEa320bF6747E18Bc0bEb2ad0950eDBB8040e9
BALANCE
100.00 ETH
TX COUNT
0
INDEX
4
ADDRESS
0x 7F0ED0D33eC2F83aD7Fd5F5D97EED2d270a7788c
BALANCE
100.00 ETH
TX COUNT
0
INDEX
5
Type here to search


METAMASK
QUICKSTART
99.987 ETH
Deposit
Send
Account 2
History
99.987 ETH
Don't see your tokens?
Add Token
Type here to search

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In this paper, we presented a solution that will replace the conventional approach of birth/death certificate generation. We have used blockchain technology and Blockcerts in the process of birth/death certification and validation. The solution includes registration of birth/death, creation of JSON file (digital certificate), public-private key cryptography to achieve confidentiality using encryption and digital signature. Moreover, the retrieval of certificates in case of certificate missing can be done easily. Furthermore, we have discussed the concept of Blockcerts, the shareability of certificate, working of blockchain technology in the process of certification. We have also discussed the key features of blockchain technology which will provide the new way of generating birth/death certificate and its validation.

5.2 Future Scope

1. Payment processing and money transfers [14]

Arguably the most logical use for blockchain is as a means to expedite the transfer of funds from one party to another. As noted, with banks removed from the equation, and validation of transactions ongoing 24 hours a day, seven days a week, most transactions processed over a blockchain can be settled within a matter of seconds.

2. Monitor supply chains

Blockchain also comes in particularly handy when it comes to monitoring supply chains. By removing paper-based trails, businesses should be able to pinpoint inefficiencies within their supply chains quickly, as well as locate items in real time. Further, blockchain would allow businesses, and possibly even consumers, to view how products performed from a quality-control perspective as they traveled from their place of origin to the retailer.

3. Retail loyalty rewards programs

Blockchain could further revolutionize the retail experience by becoming the go-to for loyalty rewards. By creating a token-based system that rewards consumers, and storing these tokens within a blockchain, it would incentivize consumers to return to a certain store or chain to do their shopping. It would also eliminate the fraud and waste commonly associated with paper- and card-based loyalty rewards programs.

4. Digital IDs

More than 1 billion people worldwide face identity challenges. **Microsoft** is looking to change that. It's creating digital IDs within its Authenticator app -- currently used by millions of people -- which would give users a way to control their digital identities. This would allow

folks in impoverished regions to get access to financial services, or start their own business, as an example. Of course, Microsoft's attempts to create a decentralized digital ID are still in the early stages [14].

More than 1 billion people worldwide face identity challenges. **Microsoft** is looking to change that. It's creating digital IDs within its Authenticator app -- currently used by millions of people -- which would give users a way to control their digital identities. This would allow folks in impoverished regions to get access to financial services, or start their own business, as an example. Of course, Microsoft's attempts to create a decentralized digital ID are still in the early stages [14].

5. Data sharing

Cryptocurrency IOTA launched a beta version of its Data Marketplace in November, demonstrating that blockchain could be used as a marketplace to share or sell unused data. Since most enterprise data goes unused, blockchain could act as an intermediary to store and move this data to improve a host of industries. While still in its early stages, IOTA has more than 35 brand-name participants (with Microsoft being one) offering it feedback.

6. Copyright and royalty protection

In a world with growing internet access, copyright and ownership laws on music and other content has grown hazy. With blockchain, those copyright laws would be beefed up

considerably for digital content downloads, ensuring the artist or creator of the content being purchased gets their fair share. The blockchain would also provide real-time and transparent royalty distribution data to musicians and content creators.

7. Digital voting

Worried about voter fraud? Well, worry no more with blockchain technology. Blockchain offers the ability to vote digitally, but it's transparent enough that any regulators would be able to see if something were changed on the network. It combines the ease of digital voting with the immutability (i.e., unchanging nature) of blockchain to make your vote truly count.

8. Real estate, land, and auto title transfers

One of the primary goals of blockchain is to take paper out of the equation, since paper trails are often a source of confusion. If you're buying or selling land, a house, or a car, you'll need

to transfer or receive a title. Instead of handling this on paper, blockchain can store titles on its network, allowing for a transparent view of this transfer, as well as presenting a crystal-clear picture of legal ownership [14].

9. Food safety

Yet another intriguing use for blockchain could be in tracing food from its origin to your plate. Since blockchain data is immutable, you'd be able to trace the transport of food products from their origin to the supermarket. What's more, should there be a food-borne illness, blockchain would allow the source of the contaminant to be found considerably quicker than it can be now.

10. Immutable data backup

Blockchain might also be the perfect way to back up data. Even though cloud storage systems are designed to be a go-to source for data safekeeping, they're not immune to hackers, or even infrastructure problems. Using blockchain as a backup source for cloud data centres -- or for any data, as **Boeing** is considering with GPS receivers on its planes -- could resolve this concern.

11. Tax regulation and compliance

Have I mentioned how important transparency and immutability are yet? For example,

marijuana companies can use blockchain as a means to record their sales and demonstrate tolawmakers that they're abiding by local, state, and/or federal laws. More importantly, these sales act as a clear record for the IRS that they've paid their fair share of taxes to the federal government, assuming they're profitable.

12. Workers' rights

Another interesting use for blockchain is as a means to bolster the rights of workers around the globe. According to the International Labor Organization, 25 million people worldwide work in forced-labor conditions. **Coca-Cola**, along with the U.S. State Department and other partners, is working on a blockchain registry complete with smart contracts -- protocols that verify, facilitate, or enforce a contract -- to improve labor policies and coerce employers to honor digital contracts with their workers.

13. Medical recordkeeping

The good news is the medical sector has already been moving away from paper for

recordkeeping purposes for years. However, blockchain offers even more safety and convenience. In addition to storing patient records, the patient, who possesses the key to access these digital records, would be in control of who gains access to that data. It would be a means of strengthening the HIPAA laws that are designed to protect patient privacy.

14. Weapons tracking

One of the hot-button topics on any news network at the moment is gun control and/or weapons accountability. Blockchain could create a transparent and unchanging registry network that allows law enforcement and the federal government to track gun or weapon ownership, as well as keep a record of weapons sold privately [14].

15. Wills or inheritances

Blockchain may also be able to put your end-of-life concerns to rest. Rather than creating a paper will, people may have the option of creating and storing their digital will on a blockchain network. When used with smart contracts, which could divvy out inheritances

based on when certain criteria are met (such as when a grandchild reaches a certain age), wills should become crystal clear and legally binding, leaving no questions as to who should receive what assets when you pass away.

16. Equity trading

At some point, blockchain could rival or replace current equity trading platforms to buy or sell stocks. Because blockchain networks validate and settle transactions so quickly, it could eliminate the multiday wait time investors encounter when selling stock(s) and seeking access to their funds for the purpose of reinvestment or withdrawal.

17. Managing Internet of Things networks

Networking giant **Cisco Systems** may be behind a blockchain-based application that would monitor Internet of Things (IoT) networks. The IoT describes wirelessly connected devices that can send and receive data. Such an application could determine the trustworthiness of devices on a network -- and continuously do so for devices entering and leaving the network, such as smart cars or smartphones.

18. Expediting energy futures trading and compliance

Even the energy industry is getting in on the act. Similar to the benefits it could bring to equity traders above, blockchain offers the ability to help energy companies settle futures

trading considerably faster than they currently do. It's also worth noting that blockchain could

help energy companies with regard to logging their resources and maintaining regulatory compliance.

19. Securing access to belongings

Smart contracts within blockchain networks also have the ability to be customized to a businesses or consumers' needs. As a consumer, you could use blockchain as a means to grant access to your house for service technicians, or allow your mechanic access to your car to perform repairs. But without this digital key, that only you possess, these service technicians wouldn't be able to gain access to your belongings.

20. Tracking prescription drugs

Finally, blockchain could be a means of transparently tracking prescription medicines. In a world where prescription returns do occur, and counterfeit medications are a real thing, blockchain offers drugmakers the ability to track their products based on serial and/or batch numbers to ensure that consumers are getting the real deal when they pick up medicine from the pharmacy. **Merck** is currently testing such a system for prescription drug returns [14].

REFERNCES

[1]. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

[2]. Bitcoin, B. (2015). BlockChain Technology.

[3]. William Bible, Jon Raphael, Matthew Riviello and Peter Taylor of Deloitte & Touche LLP, and Iliana Oris Valiente, "Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession", [online] Available: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf (accessed April 12, 2020).

[4]. Mayank, "Blockchain Technology Explained: Introduction, Meaning, and Applications", [online] Available: https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2 (accessed April 13, 2020).

[5]. Shaanray, "Merkle Trees", [online] Available: https://hackernoon.com/merkle-trees-181cb4bc30b4 (accessed April 13, 2020).

[6]. Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang, "Blockchain challenges and opportunities: a survey," Int, J, Web and Grid Services, Vol. 14, pp. 352-375, 2018.

[7]. Wikipedia, "Distributed Ledger", [online] Available: https://en.wikipedia.org/wiki/Distributed_ledger, (accessed April 13, 2019).

[8]. *Hasib Anwar, "Basic Features of Blockchain Technology", [online] Available:* https://101blockchains.com/introduction-to-blockchain-features/ (accessed April 13, 2019).

[9]. Tara Salman, Maeda Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka" Security Services using Blockchain: A State of the Art Survey," IEEE, Volume 21, pp. 1-23, 2019.

[10]. Sharma, N., Afzal, M., & Dixit, A. (2020). Blockchain-Blockcerts based Birth/Death Certificate Registration and Validation. *International Journal of Information Technology (IJIT)*, *6*(2).

[11]. *Victor Lai, "INTRODUCTION TO CRYPTOGRAPHY IN BLOCKCHAIN TECHNOLOGY", [online] Available:* https://crushcrypto.com/cryptography-in-blockchain/ (accessed April 13, 2019).

[12]. *Bernard Marr, "30+ Real Examples Of Blockchain Technology In Practice", [online] Available:* https://www.forbes.com/sites/bernardmarr/2018/05/14/30-real-examples-of-blockchain-technology-in-practice/#4b5be68f740d (accessed April 13, 2019).

[13]. *W3schools, "Blockchain Advantages and Disadvantages", [online] Available:* https://www.w3school.in/blockchain-advantages-and-disadvantages/ (accessed April 13, 2019).

[14]. *Sean Williams, "20 Real-World Uses for Blockchain Technology", [online] Available:* https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx (accessed April 13, 2019).