**Implementing Block Chain to Tackle Counterfeit in Pharmaceutical Industry**

Project Report Submitted in Partial Fulfilment of the Requirements for the Degree of

**Bachelor of Technology**

***in***

**Computer Science and Engineering**

*Submitted by*

Abhinav Gupta: (Roll No. 14101100)

Abhishek Mukhopadhyay: (Roll No. 1410110013)

Akshit Vaid: (Roll No. 1410110034)

***Under the Supervision of***

Dr. Anuradha Ravi

Assistant Professor



Department of Computer Science and Engineering

April, 2018

**DECLARATION**

I/We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Name of the Student \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature and Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Student \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature and Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of the Student \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature and Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGEMENT**

We would like to thank the Department of Computer Science and Engineering at Shiv Nadar University for giving us the opportunity to carry out this project. We would like to express our profound gratitude and deep regards for our project advisor Dr. Anuradha Ravi for her exemplary guidance, monitoring and constant encouragement throughout this project. We would also like to appreciate the constructive criticism and feedback. We would also like to thank Dr. Debopam Acharya for his help and invaluable advice. We would also like to thank our peers for their suggestions and feedback which helped us to make changes to our project and helped us to further improve it.

**TABLE OF CONTENTS**

1. Introduction

1.1. Challenges involved in tackling counterfeit

1.2. The Blockchain

1.3.1. What is Blockchain?

1.3.2. What is Block?

1.3.3. Key features of Blockchain

1.3.4. Technicalities of Blockchain

1.3.4.1. SHA256 Hash Function

1.3.4.2. Open Key Cryptography

1.3.4.3. Distributed Ledger and P2P Network

1.3.4.4. Proof of Work

1.3.5. What is Ethereum?

1.3.6. Smart Contracts

1.3.7. Ethereum Virtual Machines (EVM)

1.3.8. Decentralised Application

1.3.10. Different Blockchains available

1.3.11. Private Blockchains

1.3. Advantages of using blockchain to solve issue of counterfeit medicines

2. Literature Survey

3. Project Description and Process Flow

3.1. Parameters and their Justification

3.1. Data Flow Diagram

3.2. Context Flow Diagram

3.3. Use Cases

3.3.1. Use Case Diagram

3.3.2. Manufacturer

3.3.3. Shipper, Distributor, Retailer, Hospital and Doctor

3.3.4. Individual Customers

3.3.5. Tracking Medicine Box

4. System Architecture

4.1. Hardware

4.1.1. Arduino

4.1.2. Modules

4.1.3. Sensors

4.1.3.1. LDR Sensor

4.1.3.2. DHT22 Temperature and Humidity Sensor

4.1.3.3. PIR Sensor

4.1.4. Libraries

4.1.4.1. SD Card

4.1.4.2. SPI

4.1.4.3. DHT Library

4.1.4.4. Johny Five Javascript

4.2. Software

4.2.1. The Codrops Framework

4.2.2. The Login Page

4.2.3. For the Manufacturer

4.2.4. For the Shippers, Distributors, Retailers, Hospitals and Doctors

4.2.5. For the Individuals or Guest Users

4.2.6. The Tracking page

4.2.7. How an Ethereum Contract connects to the Network?

4.2.7.1. Testing Truffle/Mocha

4.2.7.2. Starting the application

5. Conclusion

6. Future Work

7. References

**LIST OF TABLES**

**LIST OF FIGURES**

Fig. 1.1. The addresses of various hash functions

Fig. 1.2. How open key cryptography works in a blockchain

Fig. 1.3. A view of distributed ledger

Fig. 1.4. Simplified view of Proof of Work

Fig. 1.5. Simplified view of a smart contract

Fig. 1.6. Benefits of Decentralized networks

Fig. 1.7. Proposed real-world working of project

Fig. 3.1. Data Flow Diagram

Fig. 3.2. Context Diagram

Fig. 3.3. Use Case Diagram

Fig. 3.4. Profile page for manufacturers

Fig. 3.5. Page for selling medicines

Fig. 3.6. Profile page for shippers, distributors, retailers, hospitals and doctors

Fig. 3.7. Guest option on Login page

Fig. 3.8. Field to enter medicine name and batch number

Fig. 3.9. Travel history of medicine box

Fig. 4.1. Arduino Board

Fig. 4.2. SD card module

Fig. 4.3. LDR sensor

Fig. 4.4. DHT22 sensor

Fig. 4.5. PIR sensor

Fig. 4.6. The complete circuit

Fig. 4.7. Circuit diagram of the entire circuit

Fig. 4.8. Simplified view of Ethereum nodes

Fig. 4.9. Simplified view of how solidity code is compiled

Fig. 4.10. Simplified view of how compiled solidity code is deployed

Fig. 4.11. Simplified view of the Ganache local test network

Fig. 4.12. Simplified view of Mocha testing

Fig. 4.13. Simplified view of Truffle testing

Fig. 4.14. Ganache showing accounts with full ether

Fig. 4.15. Activating truffle and lite server

Fig. 4.16. New blocks mined in ganache due to selling medicine

**ABSTRACT**

The pharmaceutical industry has always been plagued by the problem of counterfeit medicines, and with the proliferation of the internet and e-commerce, it has become very easy to procure and sell counterfeit medicines over the internet to unsuspecting customers. This market has become very lucrative (estimated value of $75 to $200 billion by the U.S. Department of Commerce) and is growing at an alarming rate ($53 million worth of counterfeit medicines seized by INTERPOL in 2016, compared to $6.3 million in 2011).

Authorities, regulators and pharma companies are adopting digital technologies like QR codes, RFID chips, Datamatrix solution of France, etc. but to limited effect due to the extremely complex chain of intermediaries through which medicines go before they reach the patient. This provides many opportunities for counterfeit medicines to enter the market, which ultimately reduces the patients’ trust for the healthcare system.

Our proposed solution is to implement a blockchain to store the travel history of every box of medicine manufactured by a company, which will be visible to all the relevant stakeholders (manufacturer, distributor, carrier, retail shops and doctors). The boxes will be fitted with sensors and microchips (smart contract) to detect on any undesirable environmental changes and store that information, which will be eventually uploaded to the blockchain upon connecting. The implementation of blockchain will allow the stakeholders to see whether the box/package has been subjected to any suspicious activity (taken off course, unauthorized access, tampering, etc.) and the location as well as personnel involved in the same. Patients are not being considered as stakeholders due to feasibility issues, especially in places like South and South-East Asia, Africa, Latin America, China, etc.

**1. INRODUCTION**

There are 2 ways in which the amount of ‘value’ associated with a person is measured, either with notes, which are usually difficult to copy objects having a particular ‘value’ associated with it (bank notes), or with ledgers, which is a list of all the transactions carried out by a person (bank passbook). But in the digital world, creating ‘notes’ is very difficult as they can be copied very easily, thus reducing their value. Thus ledgers are more practical, as long as they are immutable. This concept, termed as Blockchain has gained immense popularity and is addressed to be the next big thing after the Internet. It is an immutable ledger containing all the transactions carried out by a particular address. The most important information in blockchain includes the address of the sender, address of the receiver, the date of transaction, and the value of the transaction. All people/nodes participating in a blockchain network form a network of value, i.e. a network designed to optimize the initial creation, and further transfer of assets or ‘value’ between the participants. The reward for verifying the ledger is a certain amount of ‘value’, paid in the form of crypto-currency like Ethereum or Bitcoin. [12]

**1.1. Challenges involved in tackling counterfeit**

The counterfeit medicines market is an exceptionally notorious one due to several reasons, such as the physical harm it causes to unsuspecting and vulnerable people, economic problems for legitimate pharmaceutical companies and nations, creating drug-resistant varieties of dangerous pathogens (tuberculosis, etc.), the extremely high profit margins (sometimes over 3000%), difficulty in detecting fake medicines, weak and often complicated laws in developing countries, and very less punitive repercussions if caught (when compared to drug peddling, etc.). The total value of this illicit trade in probably in several hundred billions. The issues facing international law enforcement agencies dealing with it (like WHO’s IMPACT) include very long and complicated supply chains of the finished medicines as well as their components, the recent mushrooming of online pharmacies selling cheap medicines without prescriptions, as well as varying legal status of medicines from one country to another. Even in US, a country with some of the most stringent laws regarding medicines, there is counterfeit medicine industry valued at almost 15 billion USD. [13] [14] [15]

**1.2. The Blockchain**

**1.2.1. What is Blockchain?**

Blockchain can be known as the spine of the whole digital currency framework [25]. Blockchain innovation not just assists the clients to perform transactions utilizing cryptographic form of money, but, also ensures the security and anonymity of the clients. It is a continuously developing chain of records called blocks, which are connected and secured using cryptographic methods. A Blockchain can fill in as “an open and distributed ledger that can record transactions between two parties in a verifiable and permanent way.” This record (ledger) is shared among everybody in the system and is open for all to view. This establishes transparency and trust into the framework.

**1.2.2. What is a Block?**

A block is the 'present' some portion of a Blockchain which records a few or the greater part of the current exchanges, and once finished goes into the blockchain as perpetual database [25]. Each time a piece gets finished, another square is produced.

The Blockchain is normally run by the nodes of the network, collectively achieving on a census for approving new blocks. Once recorded, the information in any given piece can't be adjusted retroactively without the modification of every single consequent square and an arrangement of the system greater part. Exchanges once put away in the Blockchain are immutable and can't be hacked or controlled.

**1.2.3. Key features of Blockchain**

* **Public Ledgers:** The record which holds the details of all transactions which occur on the Blockchain, is open and totally available to everybody who is related with the framework [25]. When you join the Blockchain network, at that point you can download the ledger from the beginning of the network. Despite the fact that the total record is freely available, the people associated with the transactions remains totally unknown.
* **Decentralised System:** The Blockchain framework uses a decentralized approach when compared with banks and budgetary associations which are controlled and administered by Central or Federal Authorities. Here, everybody who is a piece of the framework turns out to be similarly in charge of the development and destruction of the framework. As opposed to one single element holding the power, everybody who is included with the framework holds some power.
* **Confirmation of Every Individual Transaction:** Each and every exchange is confirmed by cross-checking the record and the approval of the exchange is sent within a couple of minutes. Through the use of complex encryption and hashing techniques, the issue of double spending is also wiped out.
* **Low or No Transaction Fees:** Transaction fees are generally not applied but certain variations of Blockchain do implement certain insignificant transaction charges. These charges are however generally very less when contrasted with the expenses suggested by banks and other money related associations. If a transaction needs to move up the transaction queue, an extra expense can be included by the client in order to have the exchange done on a priority.

**1.2.4. Technicalities of Blockchain**

Some of the most important techniques used to build the blockchain and that have made this framework a revolutionary idea in various fields [25]:

**1.2.4.1. SHA256 Hash Function:**

The main hash algorithm used as a part of blockchain innovation is the SHA256. The reason for utilizing a hash is that its output doesn’t give 'encryption' i.e it can't be decrypted back to the original content. It is a 'one-way' cryptographic function, and yields same size for any size of source text. To improve understanding, let us take a gander at a case underneath:



Fig. 1.1. The addresses of various hash functions, Neel; [33]; Sep 6, 2017

As in Fig.4.1, one can see that even with the slightest of change, the algorithm yields a completely different output. But, the outputs of the hash is always of same length.

**1.2.4.2. Open Key Cryptography**

This cryptographic method helps the client by making a set of keys known as Public key and Private Key. Here the Public key is shared with others, but, the Private Key is kept as a secret by the client. To comprehend the parts of these keys, Let us take a look at the case beneath to better understand the concept:

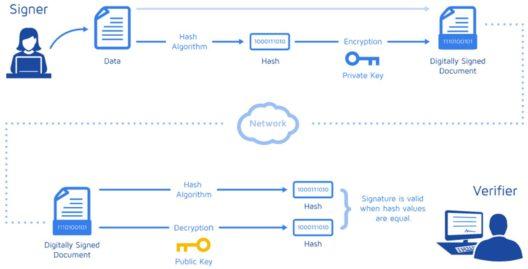


Fig. 1.2. How open key cryptography works in a blockchain, Neel;[33]; Sep 6, 2017

As in figure 1.2, if signer is sending to verifier, the signer sends the following details alongside the piece of information,

* Verifier’s address or public key.
* The information or document or cryptocurrency that Signer is sending to Verifier.
* Signer’s address or public key.

All of this information alongside a digital signature is sent through the system for confirmation. The Digital mark is again a hash made using the Signer's address and the sum he is sending to Verifier. This digital sign is encrypted with the private key. When this information reaches a miner, who needs to confirm this exchange, he follows the following steps:

* Miner takes all the un-encoded information like amount of money, public keys of both and sends it to a hash function to get a hash, in figure as hash1.
* Miner takes the digital signature and decodes it using Signer’s public key to get a hash, in figure as hash2.

If both the hashes turn out to be similar, the transaction goes through as a valid one.

**1.2.4.3. Distributed Ledger and P2P Network**

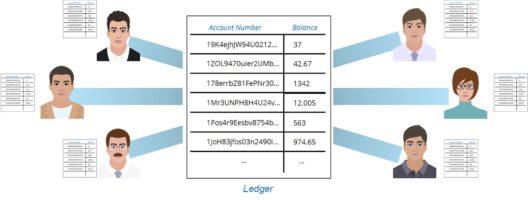
****

Fig. 1.3. A view of distributed ledger, Neel;[33]; Sep 6, 2017

Each and every individual on the system has a copy of the ledger as shown in Fig. 1.3. There is no single copy of the ledger, there are multiple. For each piece of exchanges, miners utilize hardware for computation to decrypt and arrive at a solution. More specifically, miners run the block’s metadata with a hash function. If they finds a hash that matches the present one, the miner will be granted some perks and start communicating the block over the system for every hub to approve and add to their own particular duplicate of the record. Hence, get a consensus from the network of peers rather than a central authority.

**1.2.4.4. Proof of Work**

It is fundamentally similar to solving a huge puzzle [25]. It requires loads of computational power. This work is done by individuals in the network known as miners. The trouble of the issue is balanced so that overall a block is solved within 10 minutes. Miners look for a particular nonce which gives the desired hash which is predetermined.

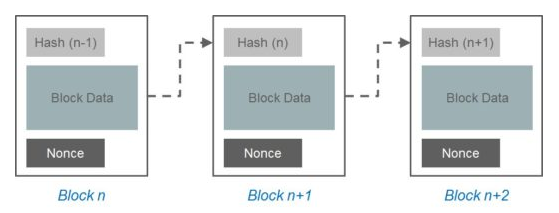


Fig. 1.4. Simplified view of Proof of Work,Neel; [33]; Sep 6, 2017

Each block has a hash value which is the mix of the previous block's hash, transaction data's hash value and the nonce. The final hash must begin with a predefined number of trailing zeroes. It is this calculation to discover the nonce which fulfills the condition that makes mining so computationally costly. So the individual who discovers this nonce is the successful miner and he/she can add their block to the blockchain. Through our P2P dispersed system, he/she communicates their block and everybody checks if hashes coordinate, refreshes their blockchain and proceeds onwards.

**1.2.5. What is Ethereum?**

Ethereum is a blockchain based decentralized platform which can be used to build decentralized applications (Dapps) and to deploy them [17]. Blockchain is the structure on which different cryptocurrencies are running on these days. Apart from providing its own cryptocurrency, ether, it also provides running of decentralized applications on its networks [19].

These applications keep running on a custom constructed blockchain, a massively intense shared worldwide foundation or infrastructure that can send value to others and accept from others, represent the owners of same.

This empowers the application developers to take advantage of it and helps them to start a venture for themselves, store registries, move finances as per guidelines given (like a will or a contract) and numerous different things that have not been invented until now, all without any intermediaries [18].

In 1994, a legal scholar and cryptographer by the name of Nick Szabo realized that these decentralized ledger can be used for implementing contracts or that later came to be known as smart contracts [18]. He proposed that the contracts can be changed to PC code, put on the framework and managed by network of users or nodes. This could likewise bring about the use of the ledger system for storing the transactions of money or receiving a product or service.

**1.2.6. Smart Contracts**

Smart contracts enables us to trade money, property, shares, or anything of significance in a transparent, conflict-free way while avoiding any kind of services provided traditionally by intermediaries [20].

The most ideal approach to describe smart contracts is to compare the mechanism with a vending machines. Usually, you would go to a legal advisor or a public accountant, pay them, and pause while you get the document. With smart contracts, you essentially drop a coin into the vending machine (i.e. record), and your product, driver’s permit, or whatever drops into your record. Also, smart contracts not just sets the rules and penalties similar to that of a normal contract does, but at the same time it also enforces these obligations.

You can utilize smart contracts for all kind of circumstances that range from money related subordinates to insurance premiums, breach of a contracts, property law, credit implementation, monetary purposes, lawful procedures and crowdfunding agreements.

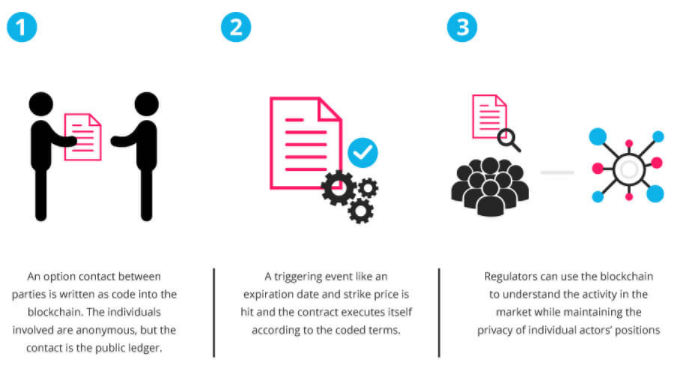


Fig. 1.5. Simplified view of a smart contract, Ameer Rosec; [34]; May,2017

Some Advantages of Smart Contracts [20]:

* **Sovereignty** - You're the one influencing the contract; there's no compelling reason to depend on a middlemen, legal counselor or different mediators to confirm. It also, rules out the possibility of control by an outsider, since execution is managed by the network of nodes, as opposed to a single authority that may be corrupt or biased.
* **Reliability** - The Automated contracts are not only less expensive but also are much faster and at the same time it also helps to avoid the errors that might occur manually.
* **Trust** - All the documents are present on the distributed ledger in an encrypted form. So, no one can tamper with it and there is no chance of losing it.
* **Safety** - Cryptography, the encryption of sites, protects your documents. There is no hacking. Truth be told, it is extremely difficult to decipher the code and make changes.
* **Data Backup** – Everyone on the network have the backup of the data. The clones of the documents are present on every users’ database.

While there can be many use cases of the smart contracts, we are using it in the healthcare sector. We are bulding smart contracts to make sure that there is no corruption or fraud happening in the supply chain of the delivery of medicines. Due to the absence of trust and transparency among the consumers, there are not many consumers buying healthcare online. This could surely help minimize it if not fully eradicate it.

As mentioned above, our Smart Contract is going to check the safety and the quality of the drugs maintained during the supply chain. This is achieved by fitting sensors into the smart box and collecting data during the transportation and checking that data across our code to declare if they are fit to consume or any tampering or quality has not been compromised with.

**1.2.7. Ethereum Virtual Machines (EVM)**

Prior to Ethereum, blockchain applications were intended to do an exceptionally limited kind of activities. Bitcoin and different forms of cryptocurrencies, for instance, were created solely to work as peer to peer digital currency sharing platform [21].

If someone wanted to create a blockchain based application, developers faced many issues. They needed to either extend the offered set of services provided by bitcoin or other cryptocurrencies which turned out to be very time consuming and tedious job for them. Alternatively they needed to develop the entire blockchain from scratch which again was not an easy task to do. So, to eradicate this issue, the founder of Ethereum, Vitalik Buterin found a new approach.

To place this into prospective, everybody can know, it is intended to fill in as a runtime environment for smart contracts based on Ethereum. This innovation can be used to automatically perform transactions or perform particular some activities on the Ethereum blockchain.

Since the Ethereum Virtual Machine is totally separated from the main network, it is a very good testing environment. Any developer hoping to make a smart contract can do so on the EVM, without it influencing the main blockchain. Testing is absolutely critical, as imperfect code can be an end for even the most exciting smart contracts. In addition, one could look at EVM as a "learning curve" to assemble greater and better smart contracts.

**1.2.8. Decentralized Applications**

Ethereum allows the developers to create and deploy decentralized applications. A decentralized application or Dapp perform some specific tasks of its clients. Bitcoin, for instance, is a Dapp that gives its clients a peer to peer cryptocurrency that allows online Bitcoin payments [22]. Since decentralized applications are comprised of code that keeps running on a blockchain network, they are not controlled by any individual or central authority.

Any service that are concentrated can be decentralized by using Ethereum. Consider all the middle person benefits that exist across different industries. From clear administrations like credits gave by banks to delegate benefits seldom considered by the vast majority like title registries, voting frameworks, administrative consistence and significantly more.

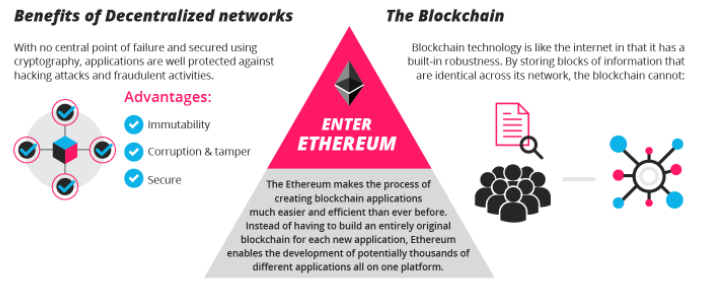


Fig. 1.6. Benefits of Decentralized networks,Ameer Rosec; [35], May,2017

Benefits of Decentralized Applications [22]:

* **Indelible** - An outsider can't roll out any improvements to information.
* **Secure** - With no main issue of central failure and secured utilizing cryptography, applications are very much ensured against hacking assaults and false exercises.
* **Defilement and Carefully Designed** - Apps depend on a system conformed to census, making hacking an impossible task.
* **Zero downtime** - Apps never go down and can never be turned off.

**1.2.9. Different Blockchains available [23]**

* **Business use of public blockchains**: Some organizations will utilize public Ethereum with their use cases that utilize a similar set of blockchain segments that they have bought or worked for their private Ethereum-based executions.
* **Consortia blockchains**: Numerous organizations have begun to develop consortia blockchains with few counterparties in their environment teaming up on few use cases to share trusted source of-truth foundation, supply or value chains.
* **Private blockchains**: Within two years, real organizations will lead to different business processes, privately and permissioned on corporate blockchains. Representatives, clients, merchants, each organization will have the capacity to safely get to that organization's private blockchain through solid cryptographically validated exchanges.

**1.2.10. Private Blockchains**

Private Blockchain is a inverse of Public blockchain. Many operations that are available to all on a public blockchains aren't open here to all. Here one can't read/write or make a transaction on the blockchain unless one has the consent to do so. In private blockchains, the proprietor of the blockchain is a single enterprise which can read write or transact on a blockchain if necessary. Thus, it can simply be known as a circulated record or database with cryptography to secure it.

In any case, it isn't too awful on the grounds that in contrast with public blockchain it is significantly speedier and less expensive on the grounds that one doesn't need to spend energy, time and cash to achieve an agreement here.

Yet, in other sense, it is substantially less secure and shut when contrasted with open blockchain in light of the fact that it can be altered/composed or perused as when wished and regarded fit by the profiting parties.

Illustration: Bankchain

In such kind blockchain:

* Not everybody can run a full hub and begin mining.
* Not everybody can make exchanges on the chain.
* Not everybody can survey/review the blockchain.

In less difficult words, to roll out any improvements in such sorts of blockchains, one needs unique privileges and accesses.

**1.3. Advantages of using blockchain to solve issue of counterfeit medicines**

We believe that one of the ways to make customers aware of the genuineness of their medicines is to allow them to see the path that their medicines have taken to reach them, starting from the manufacturer, and also whether the medicines have been exposed to any hazardous conditions during their journey (too high/low temperature, too much light, too much time, etc.) which might make them unsuitable for use. This will make the system more transparent and the various stakeholders more accountable. But we need to unsure that the information shown to the customer is genuine, and this is where blockchain comes in. The decentralised nature of this technology makes it extremely secure. Also, here we will be utilising a private blockchain, which will ensure that no unauthorised people are given permission to modify the blockchain. This will make our system very robust. The medicine boxes will contain sensors to detect temperature, pressure, light, and unauthorised entry, and the data collected will be uploaded to the blockchain in the form of a block, when the box is connected by an authorised person. The miner will get some ether for this job. Work in this area is also being done by a consortium of companies which include IBM, Cisco, etc. The way in which we have visualised our project to work in the real world is shown in the diagram below.

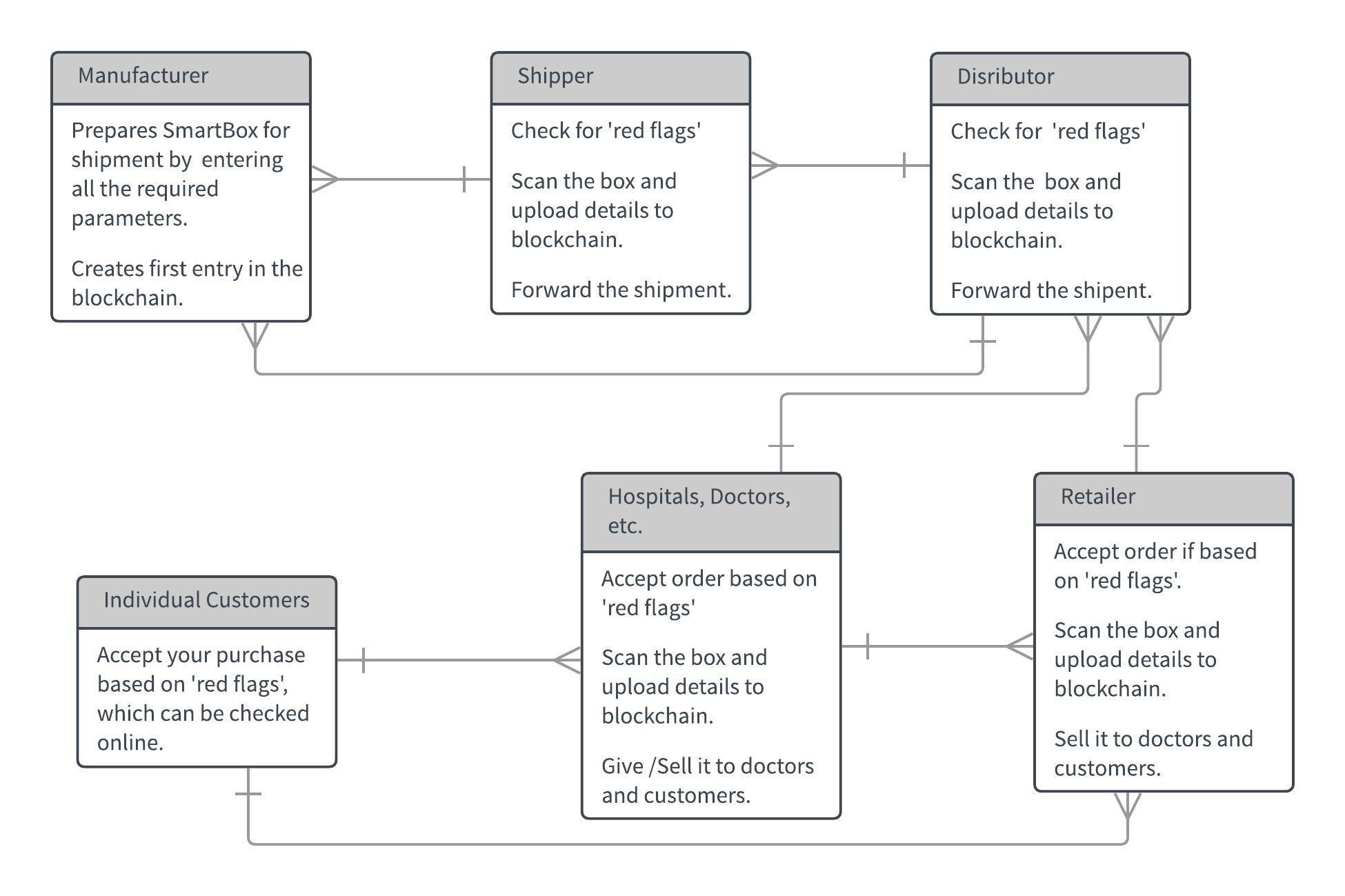


Fig. 1.7. Proposed real-world working of project

The shippers, distributers, retailers, hospitals, etc. (except the individual customers) will be able to return the SmartBox to the manufacturer after they have opened it or have rejected its contents.

**2. LITERATURE SURVEY**

The paper by Yonatan Sompolinsky and Aviv Zohar et al. [1] focused on suggesting some of the downsides or limitations of the then most populer blockchain based cryptocurrency known as bitcoin. This paper was also considered as an early motivation of developing the ethereum platform by improvising current algorithms used by bitcoin. Not only did they point out the negatives but also presented with their own set of algorithms and solutions that can possibly help in improving the platform. These negatives included mentioning the effect of network delays which happens while performing any transaction. There is a mention of how the proposed algorithm that put a bound on the amount of transactions that the network will able to handle securely. And to remove these bounds they suggested to change the available way of storing the transaction details that bitcoin uses. Their suggestion includes the use of different data structure to store the transaction information. They were the first to suggest to use hashes of the available transaction information and store the hashes onto the block unlike the entire records. They suggested a blockchain which could be way faster and secure in creation of blocks per second than the available data structure of bitcoin.

According to Satoshi Nakamoto et al. [2] in a framework of sending/receiving of money, there are many issues some due to misuse of authority by central figures,  some due to middle men, charging high amount of money against services, issue of double spending and some due to online frauds. The author proposes a secure way for exchanging digital currency amongst peers in a safe and highly secure manner. In a broad sense, he proposes to give a decentralized framework in which the exchanges can be checked and validated by all the peers present in the network, with no central authority. The records of the considerable number of exchanges are composed electronically in a digital document. This database of exchanges between peers is also known as a ledger. Each transaction is checked and confirmed only after having a consensus of the nodes which they arrive at by performing proof-of-work. After each exchange, a key is created and attached as a marker to the exchange, which is further hashed with the private key of the peer that is paying and public key of the peer that is receiving. By the use of hash functions, public key cryptography, distributed ledger, peer-to-peer network and proof of work, it makes sure that the platform is safe and sound. This is achieved by showing that it is almost impossible to forge a transaction, and looking into the effects of network delays on the transactions. And finally it shows the ideal way of storing transactions and to ways of negating the mentioned shortcomings.

The proposed platform, Ethereum by Dr. Gavin Wood et al. [3] is an upgradation over cryptocurrencies. It has new features like on-blockchain escrow and limit on exchanges. It is having the similar peer to peer policy is similar to that of other cryptocurrencies, however they have used  "Greedy Heaviest Observed Subtree" (GHOST) protocol as a modification to the available protocol. This protocol was first mentioned by Yonatan Sompolinsky and Aviv Zohar et al. [1]. It also has its own cryptocurrency known as ether. However his work is not limited to digital currency, it is also intended to create a new platform for building decentralized applications, giving an alternate arrangement of tradeoffs that can turn out to be helpful for many kinds of decentralized applications, with special focus on cases where less time, security for applications, and the capacity of various applications to communicate is critical. Ethereum does this by building a blockchain which comprised of Turing-complete programming language, enabling anybody to compose smart contracts and decentralized applications where they can make their own principles or rules for possession, exchanges and transactions. Smart Contracts, allow the transactions to take place it certain conditions are met.

The proposed idea by Guy Zyskind, Oz Nathan amd Alex ‘Sandy’ Pentland et al. [4] Privacy of the client information, that is held by centralized corporations to give customized services, was a developing concern. Legitimate frameworks didn’t exist to handle the common privacy issues of the users. A larger part of the current systems turned out to be defenseless. This paper suggests an answer where the client's information regarding its identity is added to a blockchain. Authors are basically suggesting that the blockchain data structure can have two types of transactions, one that gives access to control the administration and another one for information stockpiling and recovery. The additional information is added to blockchain by means of another type of transaction which updates the information to a key-value store. The client can grant authorization to organizations or users to get to this information, and can change or renounce these consents by means of an access call. This enhances the security and the simplicity of controlling the protection settings. The information to be included is stored using Distributed Hash table. The blockchain just contains a pointer to the information, hence, helping to secure user information in a better manner. This would thus be able to help in controlling access of a client's information by organizations.

In their research work, Jason Spasovski and Peter Eklund, et al. [5] mention about their implementation of a private consortium blockchain named Tendermint. Assuming that Proof of Stake is a more efficient alternative to Proof of work where no mining is required to achieve consensus but instead the next node to create a block is selected proportional to its stake in the blockchain, the choice of Tendermint is explained as it is a relatively lightweight blockchain solution since its consensus method is proof of stake using a voting mechanism as opposed to the more computational expensive proof of work. The tests have been carried out taking two scenarios. Each of them have the goal of simulating a large number of users simultaneously communicating via the application. The first test applies a messaging pattern based on a scale-free network. The second scenario simulates a scenario where a single node receives messages from the entire client-network. Both blockchain and non-blockchain implementations are tested for both the scenarios. Their results show that the blockchain implementation scales linearly as the number of instances is increased uptil a breakeven point. They state, about the outcomes of using the Tendermint blockchain, that it incurs a 4-8 multiplicative factor on scalability, and a multiplicative factor of 2-4 on the average response times.

Konstantinos Christisdis and Michael Deveskiotis, et al. [6] through their work, advise not to use the same blockchain for all transactions if another participant might get a competitive advantage by tracking the device’s activity. Minimization of the exposure of the deviceis recommended by setting up blockchains only with those entities and only on those processes that it needs to collaborate with and on, respectively. However, it has trade-offs between the coordination cost compared privacy and is hypothetical for different implementations. Selection of the set of miners is also discussed pertaining to the limited tolerance of consensus mechanism against Byzantine fault tolerant nodes. If the number of miners that conspire violates that threshold, the risk of transaction censorship is severe. The nodes of the mining set need to be selected wisely so that the chances of collusion between them are minimized. In a private network, legal contracts should be signed so that collusions are penalized appropriately.

Ali Dorri, Salil S.Kanhere, and Raja Jurdak, et al., [7] present various examples projects and products of IoT and BlockChain implementations. Additionally, they describe a couple of ways to store access and monitor data in a cloud based IoT environment though they abstain from naming them particularly. They compare the implementation of the Bitcoin BC and the BC employed in different tiers of their proposed architecture. It incorporates different parameters based on which comparison is made among local Blockchain, Shared Blockchain, Overlay Blockchain and the much discussed Bitcoin Blockchain. A study of the threats pertaining to the Blockchain implementation in IoT enlists the type-categorized threats along with the list of possible threats.

Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, et al. [8] present six steps that they have incorporated in their proof of stake system developed by them. The problem of realizing a proof-of-stake based Blockchain protocol is formalized in terms if persistence and liveness, which are stated as essential for a transaction ledger. The blockchain protocol developed takes into account the possibility that stake might over time. Instead of simply relying on a system of coin flipping simulation to incorporate uncertainty in the form of entropy, snapshots of the current set of stakeholders are recorded in from which randomly selected are the set of stakeholders responsible for the coin flipping protocol. A reward mechanism has also been taken care of in order to incentives. This, they claim to have proved is in accordance with the Nash Equilibrium and tackles attacks like selfish mining and block withholding which hamper smooth running of the system. For scaling up, emphasis has been made on delegation, a mechanism for revoking one’s delegated appointment as per their own wish thus, simulating liquid democracy. Even our model and protocol description we also explore how various attacks considered in practice can be addressed within our framework. A discussion of double spending attacks, transaction denial attacks, 51% attacks, nothing-at-stake, desynchronization attacks among other attacks. Time is divided into discrete units called slots. The ledger associates, with each time slot, one ledger per block. All participants have clocks at their disposal that indicate the current slot. This allows for a distributed protocol intending to collectively assign a block to this current slot. The current slot is determined by a publicly-known and monotonically increasing function of current time. Each participant has access to the current time. Any discrepancies between parties’ local time are insignificant in comparison with the length of time represented by a slot. The length of the time window that corresponds to a slot is sufficient to guarantee that any message transmitted by an honest party at the beginning of the time window will be received by any other honest party by the end of that time window. The persistence property is based on stability of transactions. Stability is parametrized and a transaction is only considered valid if it is residing in deeper than the parameter’s value. Whence stabilized, other nodes will either report in the same position in the ledger or they will not report as stable any transaction in conflict to this particular transaction. If all nodes in the system attempt to include a certain transaction, then it will declared stable after the duration equal to transaction confirmation time has been passed and will display so upon querying.

The paper by Abdulaziz Fahad Abdulaziz Alghannam, Zoe Aslanpour, Sara Evans and Fabrizio Schifano, et al. [9] focused on the issue of non-availability of detailed accounts on the current nature of the problem of counterfeit and substandard medicines and on identifying limitations in knowledge regarding counterfeit medicines in terms of geographical location, classes of medicines, and types of analysis performed on the medicine samples. Articles that reported investigations of counterfeit and substandard medicines were systematically reviewed. Articles were chosen from the records available on databases like PubMed, Scopus and ISI Web of Knowledge. Prospective studies performing chemical analysis on medicine samples were identified using the key search terms ‘counterfeit’ or ‘substandard’ and ‘medicine’ or ‘drug’ or ‘pharmaceutical’. Several issues have been highlighted, like the fact that the focus of most studies have targeted developing countries in Africa, especially Nigeria and Ghana, and Asia, especially South Asia, South-East Asia and China. But this problem of SSFFC (Substandard/Spurious/Falsely labeled/Falsified/Counterfeit) medicines in the market is equally severe in Middle Eastern countries and in South America. For example, in Yemen 32% of selected antimalarial medicines failed analysis tests, and in Egypt, Lebanon, Jordan and Saudi Arabia, 50% of the antibiotic amoxicillin was substandard, i.e. having lower API% than what is accepted by pharmacopeial limits. Also, a study in seven South American countries found 11% of antimalarials to be substandard using basic TLC chemical analysis. Also, most of the studies focused on antibiotics and other similar medicines, especially for diseases like malaria and tuberculosis. Medicines used to treat noninfectious diseases, known as non-communicable disease (NCD) medicines, or medicines for chronic diseases like diabetes, cancer, obesity, etc. were only found in a few studies. However, on a global scale, NCD medicines must not be ignored because according to WHO estimates, NCDs kill about 36 million people every year, of which about 29 million deaths, or about 80%, occur in low-income and middle-income countries.

The paper by Jakkrit Kuanpoth, et al. [10] about the problem of counterfeit medicines in Cambodia, Vietnam and Thailand focuses on the factual and legal issues surrounding counterfeit drugs in the 3 South-East Asian countries mentioned previously, in an attempt to determine the magnitude and characteristics of the drug counterfeiting problem within this region. It discusses the extent of the problem, the adequacy and effecacy of the existing laws in these countries that regulate the distribution and marketing of medicines, the concept and definition of counterfeit drugs in order to avoid variations in the legal interpretation and implementation and the issues of law enforcement and border controls. The counterfeit drugs found in this region include antibiotics, anti-malarial agents, anti-tuberculosis drugs, anti-retroviral agents, vitamins, painkillers, hormones, and steroids. Particularly, the quantities of available fake artesunate, a drug for the treatment of multi-drug resistant Plasmodium Falciparum malaria, are extremely high in this region and were found in Cambodia, Laos, Myanmar, Thailand and Vietnam. According to a 2001 survey, among 104 samples bought from shops in those five countries, 30 samples (29%) were contained no artesunate and 39 samples (38%) were counterfeit. A more recent study has shown similar results. The main problem affecting the law enforcement agencies in these countries who are trying to disrupt the counterfeit medicines market are the weak punitive sanctions against guilty people, which are acceptable to criminals as the profits from this trade ae very high, lack of government willpower, lack of resources in terms of manpower, finances and logistics, and outdated regulations.

The paper by Veronica Li and Silas Webb, et al. [11] focusses on the issue of counterfeit medicines in Sub-Saharan African (SSA) countries, and on some of the solutions which can be implemented. According to the World Health Organization (WHO) almost 50% of the medicines sold in SSA countries are fake, compared to only about 1% in the developed world. Also, the type of drugs counterfeited differs from developed countries to developing countries. In the developed countries, counterfeiters focus on expensive life-style medications such as anti-allergic agents, Viagra, weight-loss medication, etc. However, in the developing countries, counterfeiters target life-saving drugs for diseases like malaria, human immune deficiency virus (HIV), tuberculosis (TB), etc, as these diseases still affect huge numbers of people in these countries. Thus, counterfeit medicines end up playing a major role in magnifying global health inequalities. Over 90% of worldwide malaria deaths occur in Africa. This has created a huge market for criminals to produce counterfeit anti-malarials in the region. In addition, in 2006, the WHO changed the official guidelines for treating malaria to Artemisinin Combination Therapy (ACT), which although more efficient than chloroquine, costs about 5 to 23 times as much to manufacture. Thus, this market has become particularly lucrative for counterfeiters. A survey by Nayyar published in the Lancet found that 35% of 2297 anti-malarials sampled from across SSA were of sub-therapeutic quality. The situation acerbated due to inefficient regulatory bodies, weak laws, weak punitive sanctions for counterfeiters, lack of resources (manpower, finances) and corruption.

**3. PROJECT DESCRIPTION**

Our application is composed primarily of 3 components, a hardware component i.e. the SmartBox, and 2 software components i.e. the Ethereum blockchain and the UI. Data input is taken from the sensors of the SmartBox upon connection. Data is also entered by the manufacturer when preparing the SmartBox to carry a particular category of medicines. Data output is given on a screen when a user logs in to the system and connects the SmartBox to the system, or when a customer enters the Batch No. of the medicine.

**3.1. Parameters and their Justification**

**Temperature:** This parameter is used to check if the data that is collected from the sensor is below the maximum temperature. If the temperature is below the maximum temperature, implies that the efficacy of the medicine is still intact.

**Humidity:** Similar to the temperature parameter, the only difference is that it is used to maintain the ideal humidity of the medicine. To make sure that it doesn’t go stale

**Light Intensity:** This is used to make sure that the medicine is not under direct sunlight. And at the same time it can be used to make sure that the box is not opened at any point of time.

**PIR:** This is used to ensure that the box has not been tampered with, or opened by an unauthorized person. The sensor records if something blocks its line of sight.

**Location:** To track the location of the box at regular intervals of time. The purpose is to check if the box has been on course or has gone off course.

**Timestamp:** This parameter is used to keep the timing along the delivery of the medicines.

**Batch Number:** It is used in combination with the name of the medicine to keep track of the origins of the drug. It is given by the manufacturer and consumers can use it to check the details of the medicine received.

**Medicine Name:** It is used in combination with the batch number of the medicine to keep track of the origins of the drug. It is given by the manufacturer and consumers can use it to check the details of the medicine received.

**3.2. Data Flow Diagram**

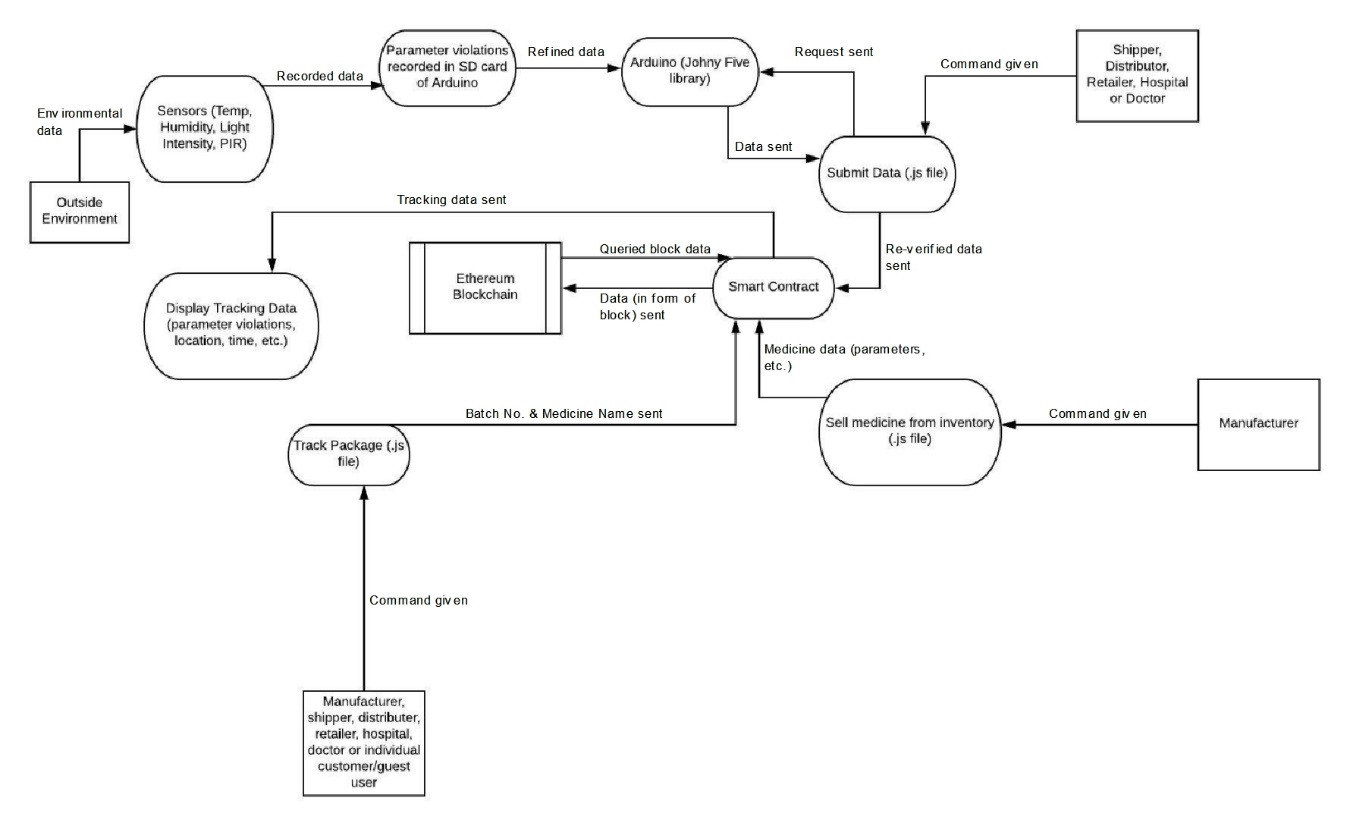
****

Fig. 3.1. Data Flow Diagram

**3.3. Context Flow Diagram**

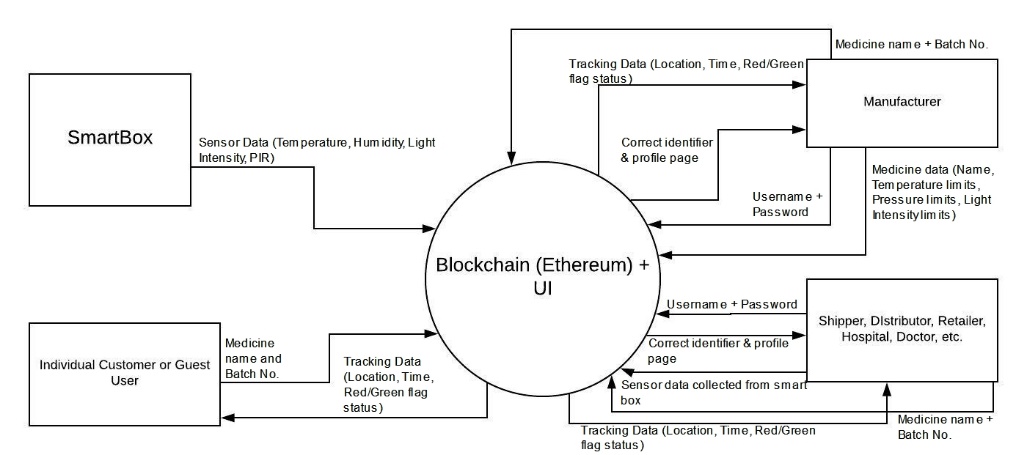
****

Fig. 3.2. Context Diagram

**3.3. Use Cases**

The project is designed to be used several types of people, namely manufacturers, shippers, distributers, retailers, hospitals, doctors and individual customers. Each of these type of people will use it for different purposes.

**3.3.1. Use Case Diagram**

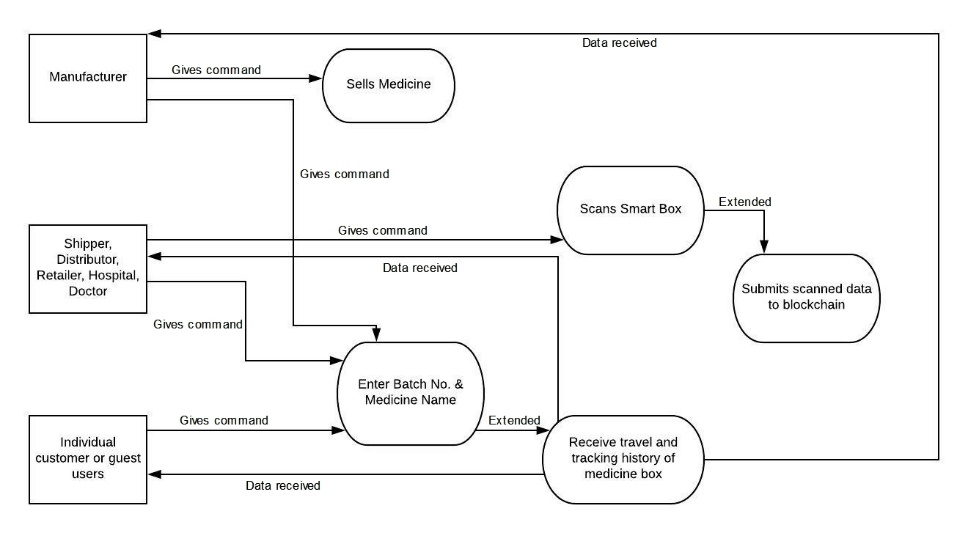
**s**

Fig. 3.3. Use Case Diagram

**3.3.2. Manufacturer**

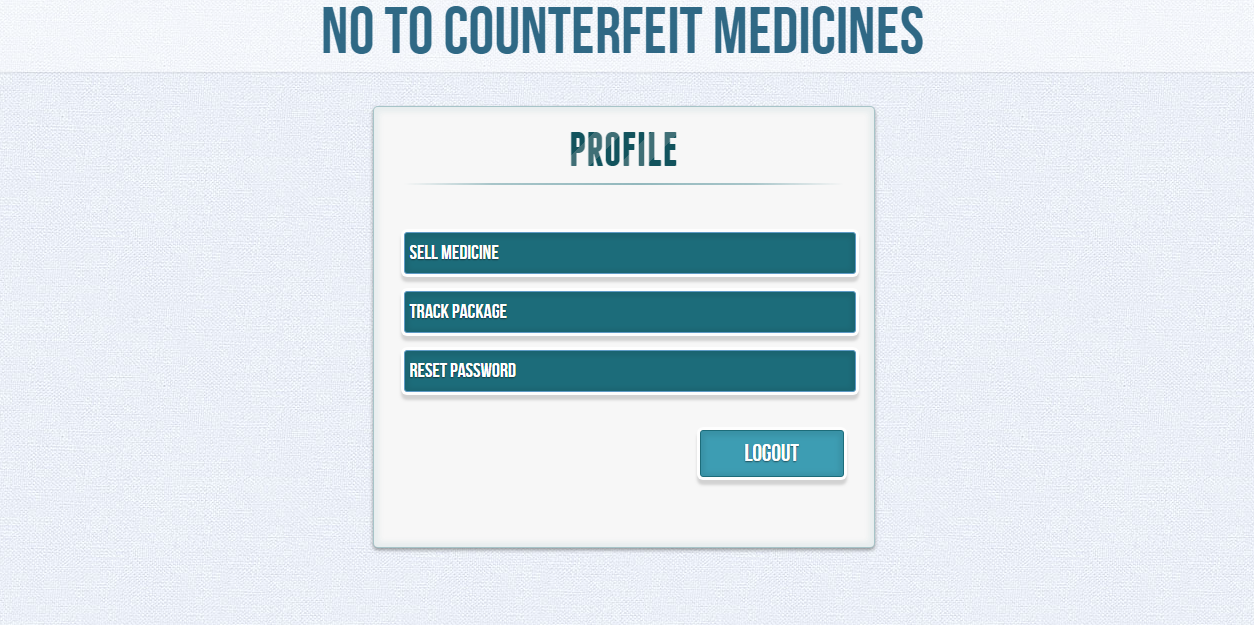
****

Fig. 3.4. Profile page for manufacturers

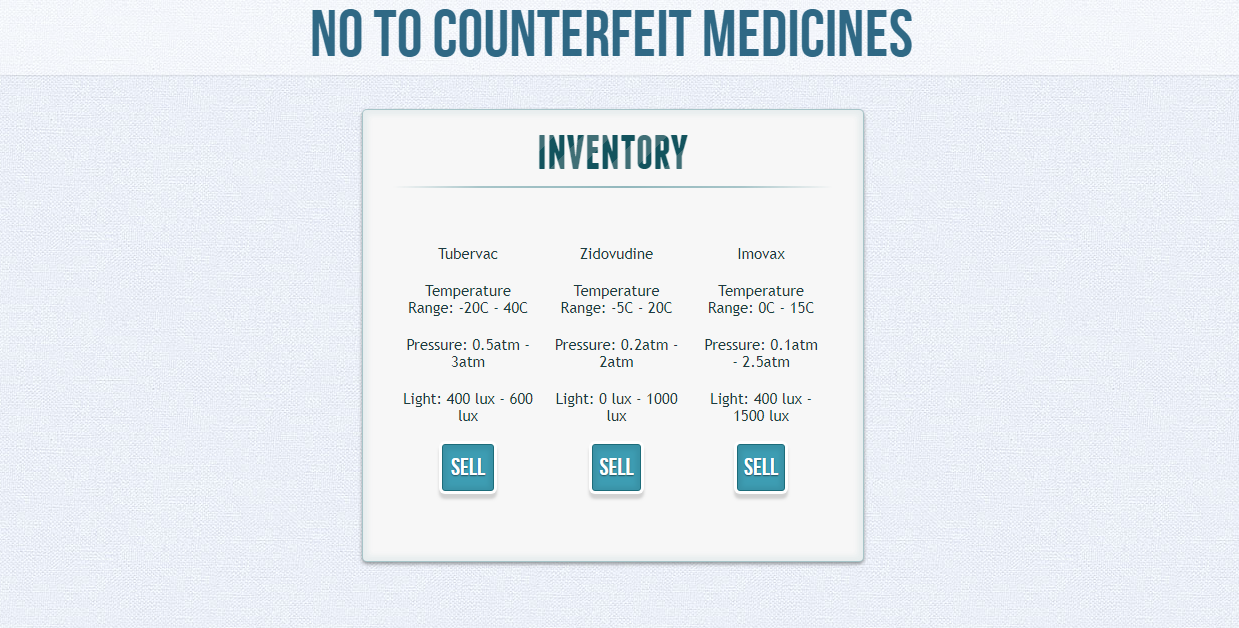
****

Fig. 3.5. Page for selling medicines

**3.3.2. Shipper, Distributor, Retailer, Hospital and Doctor**

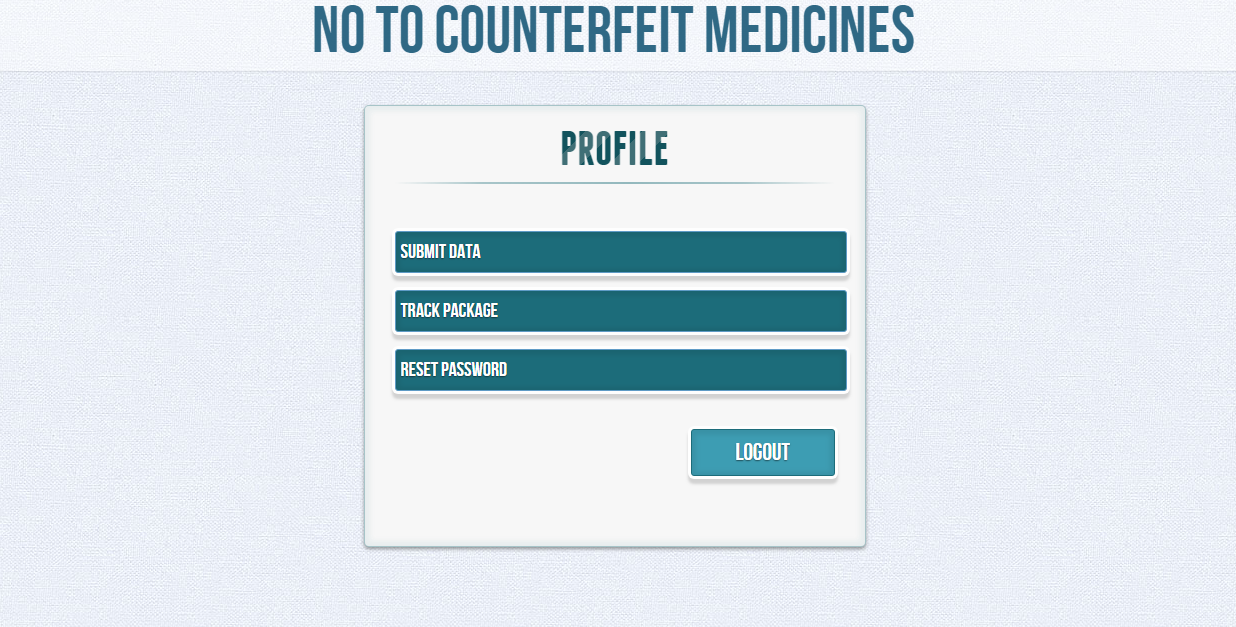


Fig. 3.6. Profile page for shippers, distributors, retailers, hospitals and doctors

**3.3.3. Individual Customers**

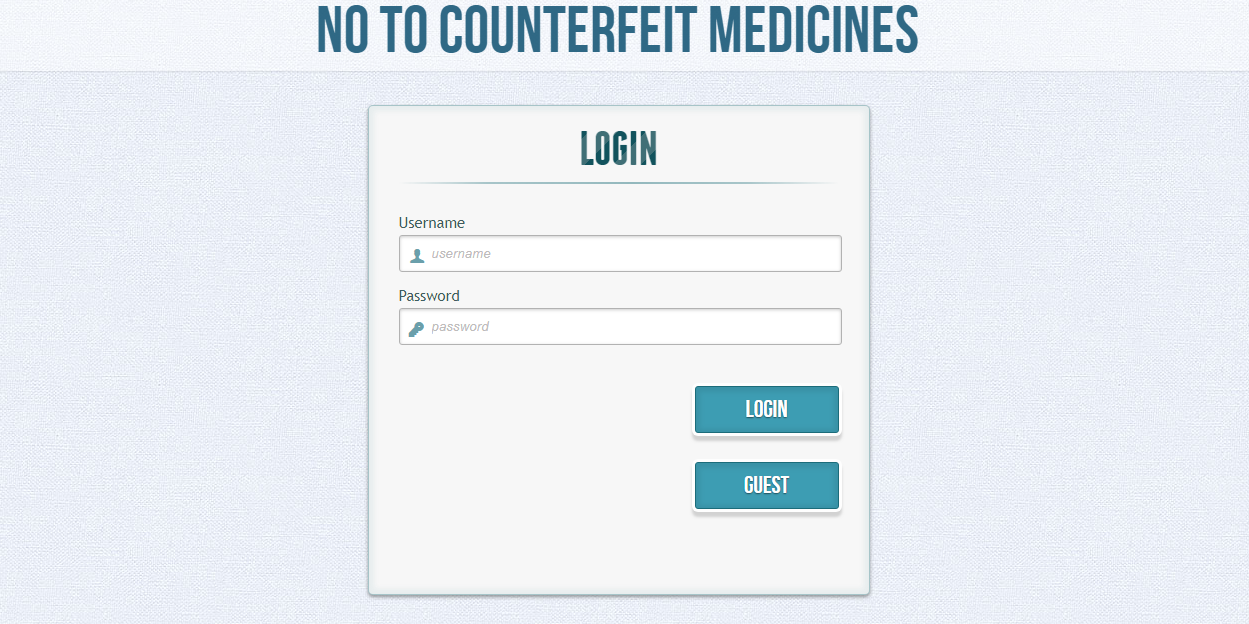


Fig. 3.7. Guest option on Login page

**3.3.4. Tracking medicine box**

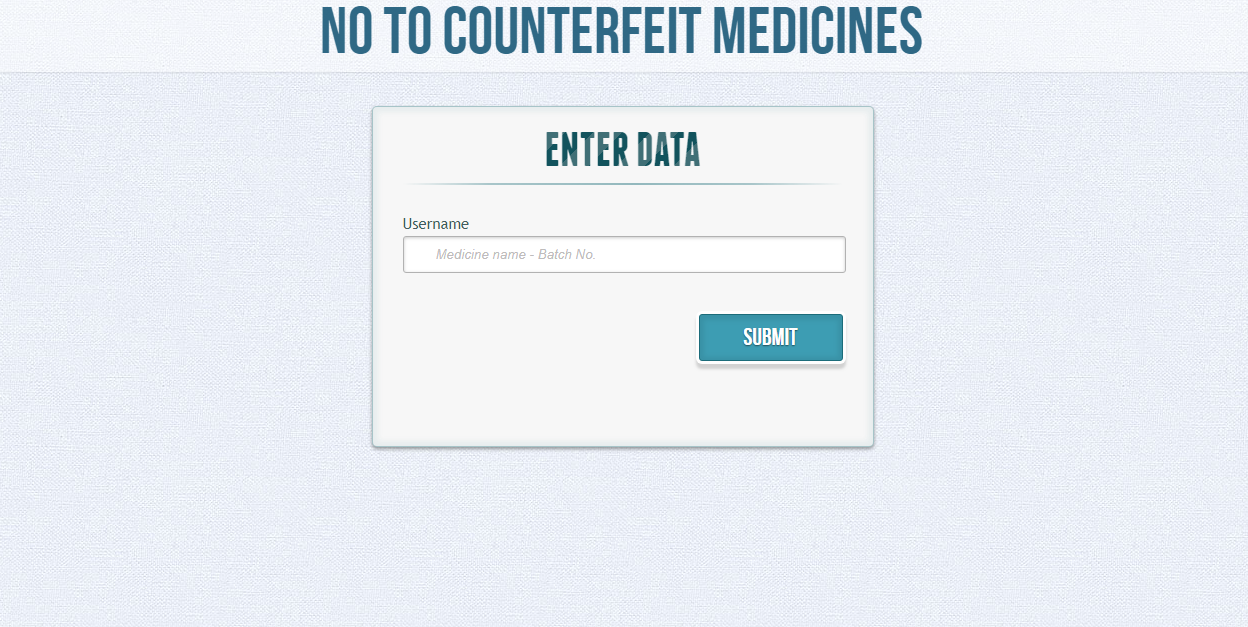
****

Fig.3.8. Field to enter medicine name and batch number

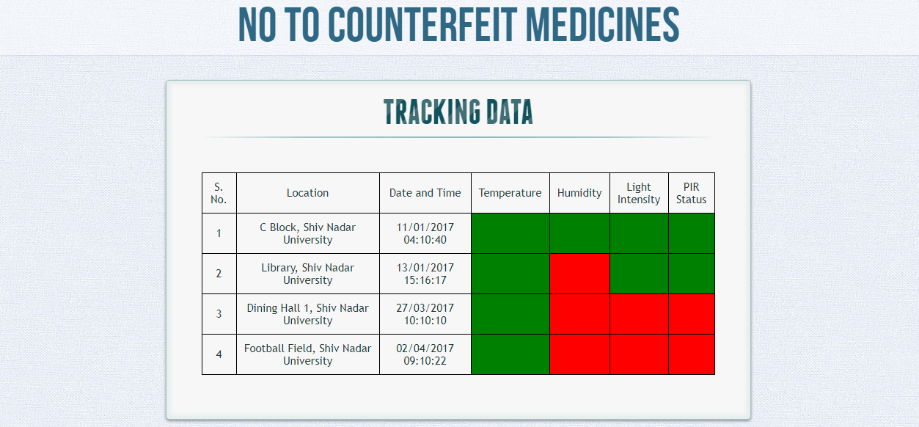


Fig. 3.9. Travel history of medicine box

**4. SYSTEM ARCHITECTURE**

The entire system is composed of 3 main parts, namely the hardware, the user interface and the blockchain.

**4.1. Hardware**

**4.1.1. Arduino**

Arduino is a microcontroller platform which allows Arduino development boards to be programmed and reprogrammed. It uses for Arduino IDE for building the code to be uploaded onto the development board. Arduino is derived from microcontrollers which consist of a standalone single chip integrated circuit, ROM to store the program and RAM for its execution along with some I/O buses. The development board consists of either Atmel ARM or Atmel AVR microcontrollers. This platform was launched to provide an easy way and an affordable platform for students and professionals to develop projects with devices that interact with their environment using sensors and actuators.

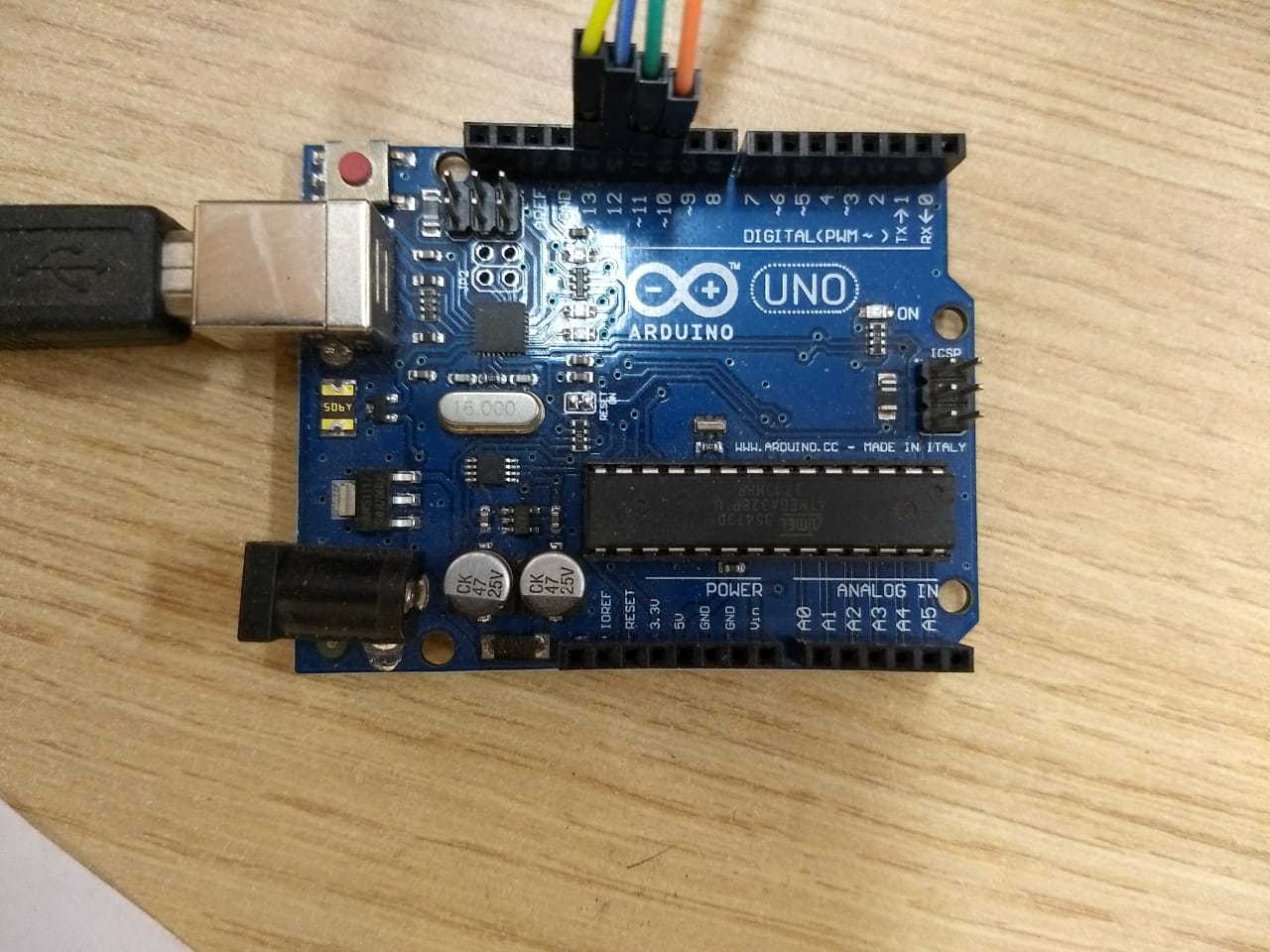


Fig. 4.1. Arduino Board

**4.1.2. Modules**

* **Arduino SD Card Module** - The Arduino SD Card Module is used to connect an external SD Card to the Arduino development board and hence provides data storage functionality to the . The module holds an SD Card Reader in which the SD Card resides and has 6 male pins to connect to the main board in order to use it.
* **Arduino PIR Module** - The Arduino PIR Module holds the PIR sensor which is used to detect the presence of any human body within a certain range [32]. It also incorporates potentiometers which allow varying the sensitivity of the PIR sensor. There are 3 male pins present in the module to connect to the microcontroller.

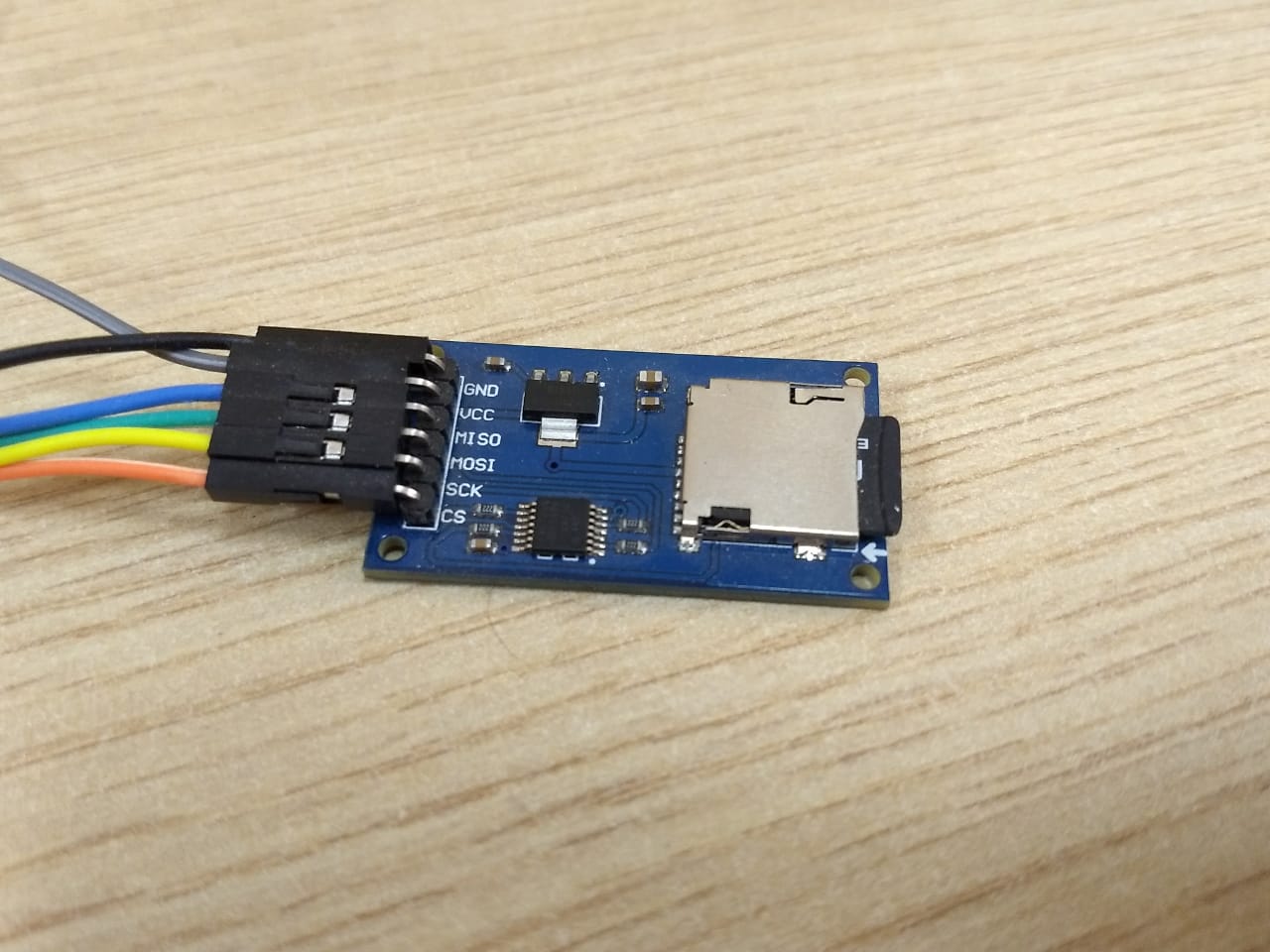
****

Fig. 4.2. SD card module

**4.1.3. Sensors**

**4.1.3.1. LDR Sensor**

This Light Dependent resistor allows the circuit to sense the presence of ambient light in the surrounding. It consists of a light sensitive diode which decreases the resistance of the LDR sensor in the presence of ambient light thus allowing the circuit to detect light. This sensor has been implemented to detect undesirable exposure to light in case of substances which are Photo-active and/or Photo-reactive substances.



Fig. 4.3. LDR sensor

**4.1.3.2. DHT22 Temperature and Humidity Sensor**

This sensor enables the circuit to obtain the temperature and level of humidity in the surroundings. It consists of an NTC thermistor which reads the data from the surroundings [29]. The operating voltage of this sensor is from 3 to 5 volts, while the max current used when measuring is 2.5mA. The DHT22’s temperature measuring range is from -40 to +125 degrees Celsius with +-0.5 degrees accuracy. Also the DHT22 sensor has a good humidity measuring range, from 0 to 100% with 2-5% accuracy.

For measuring humidity they use the humidity sensing component which has two electrodes with moisture holding substrate between them. So as the humidity changes, the conductivity of the substrate changes or the resistance between these electrodes changes. This change in resistance is measured and processed by the IC which makes it ready to be read by a microcontroller.

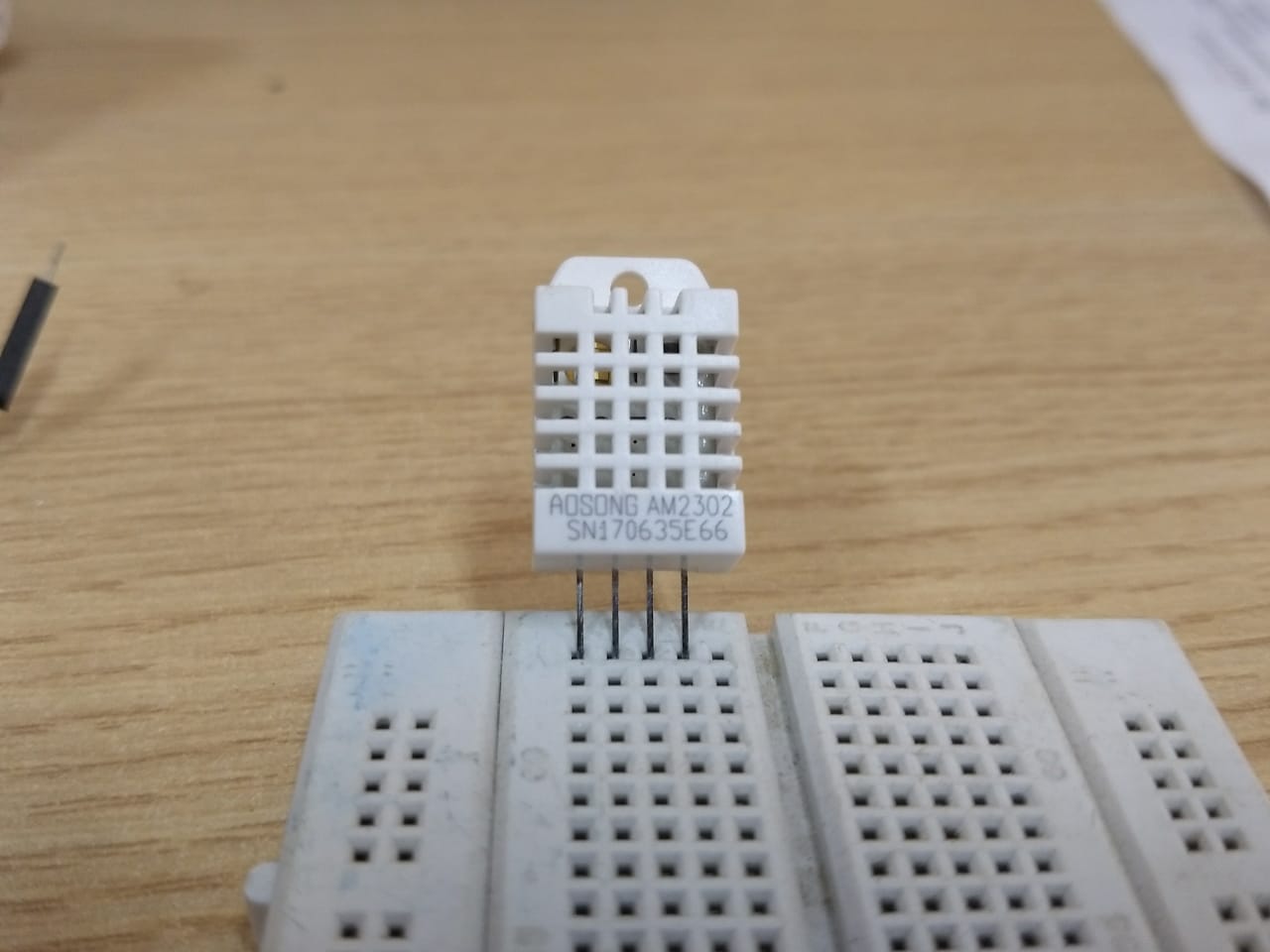


Fig. 4.4. DHT22 sensor

**4.1.3.3. PIR Sensor**

PIR sensors are used to sense motion, almost always used to detect whether a human has moved in or out of the sensors range [32]. They are small, inexpensive, low-power, easy to use and don't wear out.

PIRs are basically made of a pyroelectric sensor which can detect levels of infrared radiation. Everything emits some low level radiation, and the hotter something is, the more radiation is emitted. The sensor in a motion detector is actually split in two halves. The reason for that is that we are looking to detect motion, a change, and not average IR levels. The two halves are wired up so that they cancel each other out. If one half sees more or less IR radiation than the other, the output will swing high or low.



Fig. 4.5. PIR sensor

**4.1.4. Libraries**

**4.1.4.1. SD Card**

The SD library allows for reading from and writing to SD cards, e.g. on the Arduino Ethernet Shield. It is built on Sdfat. SdFat assumes chip select for the SD card is the hardware SS pin [26]. The library supports FAT16 and FAT32 file systems on standard SD cards and SDHC cards. It uses short 8.3 names for files [31]. It assumes chip select for the SD card is the hardware SS pin.

**4.1.4.2. SPI**

Serial Peripheral Interface (SPI) is a protocol which is used for interacting with several devices while maintaining synchronization [27]. It can be used for connecting one or more hardware modules, shields and other microcontrollers.

With an SPI connection there is always one master device, say a microcontroller, which controls the peripheral devices. Most of the SPI connections have the following lines:

* *#MISO (Master In Slave Out) - The Slave line for sending data to the master,*
* *MOSI (Master Out Slave In) - The Master line for sending data to the peripherals,*
* *SCK (Serial Clock) - The clock pulses which synchronize data transmission generated by the master and one line specific for every device.*
* *SS (Slave Select) - the pin on each device that the master can use to enable and disable specific devices.*

*#* [27]

A slave module’s pin state is used to make it communicate with its master to make it work with more than one SPI devices. When it’s low, it communicates with the master and ignores when it’s high.

**4.1.4.3. DHT Library**

The DHT library is used for its function which can compute the heat indices from the data received from the DHT22 temperature and humidity sensor. The results are usually displayed in the serial monitor but our implementation is that these are stored on an external storage [30] [29]. The data is read from the sensors and is stored in cases it goes out of the specified ranges.

**4.1.5 Communication Using Serial connections**

The data collected from the sensors and logged on to the SD card is retrieved and transferred using serial connections. The output is stored in the form of csv files which is then read using functions from a Javascript file.

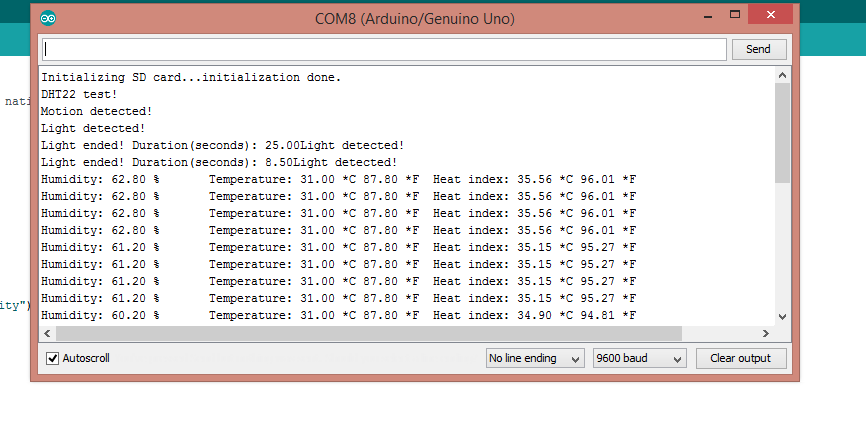


Fig. Output from the sensors on the Arduino Serial Monitor

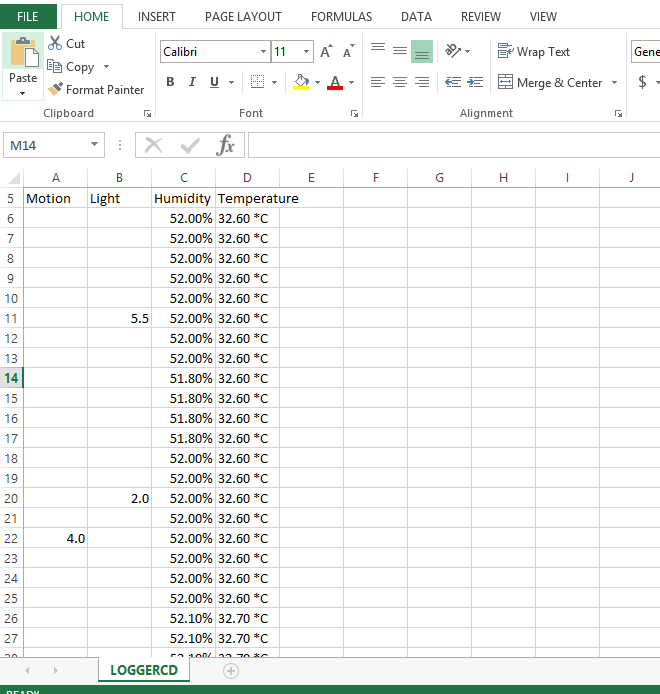


Fig. Data Retrieved in the from CSV Files

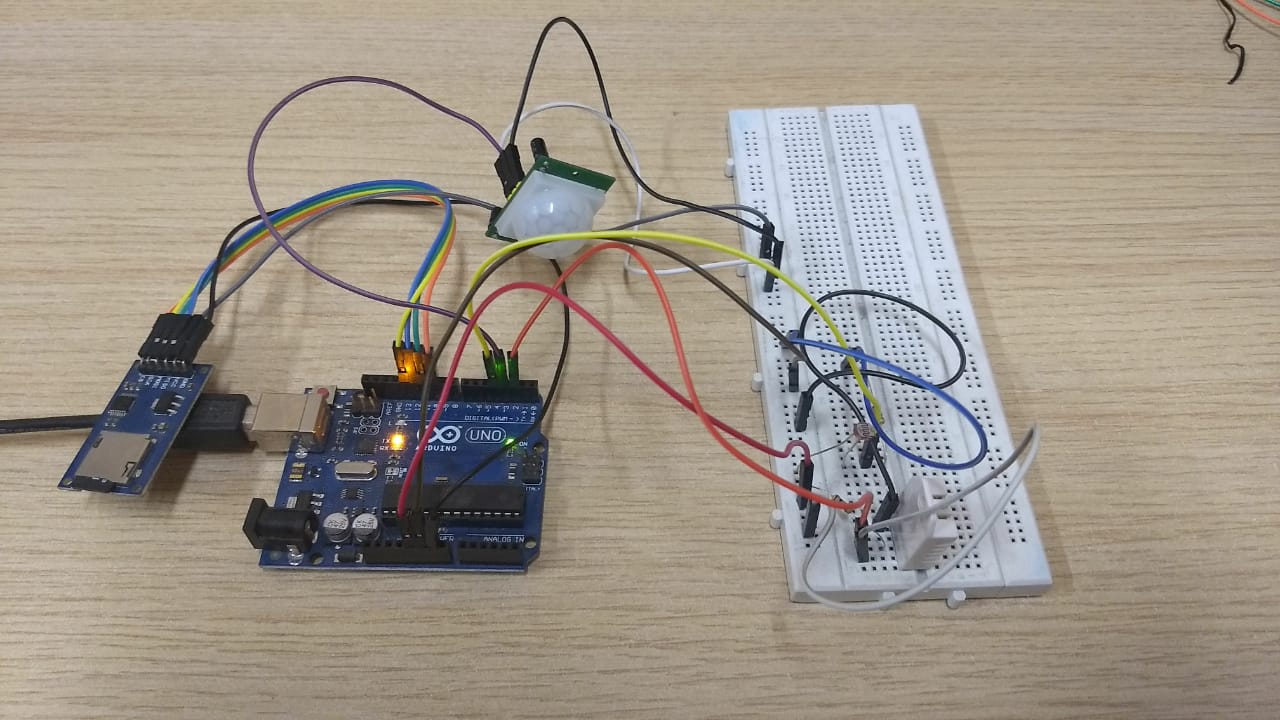
****

Fig. 4.6. The complete circuit

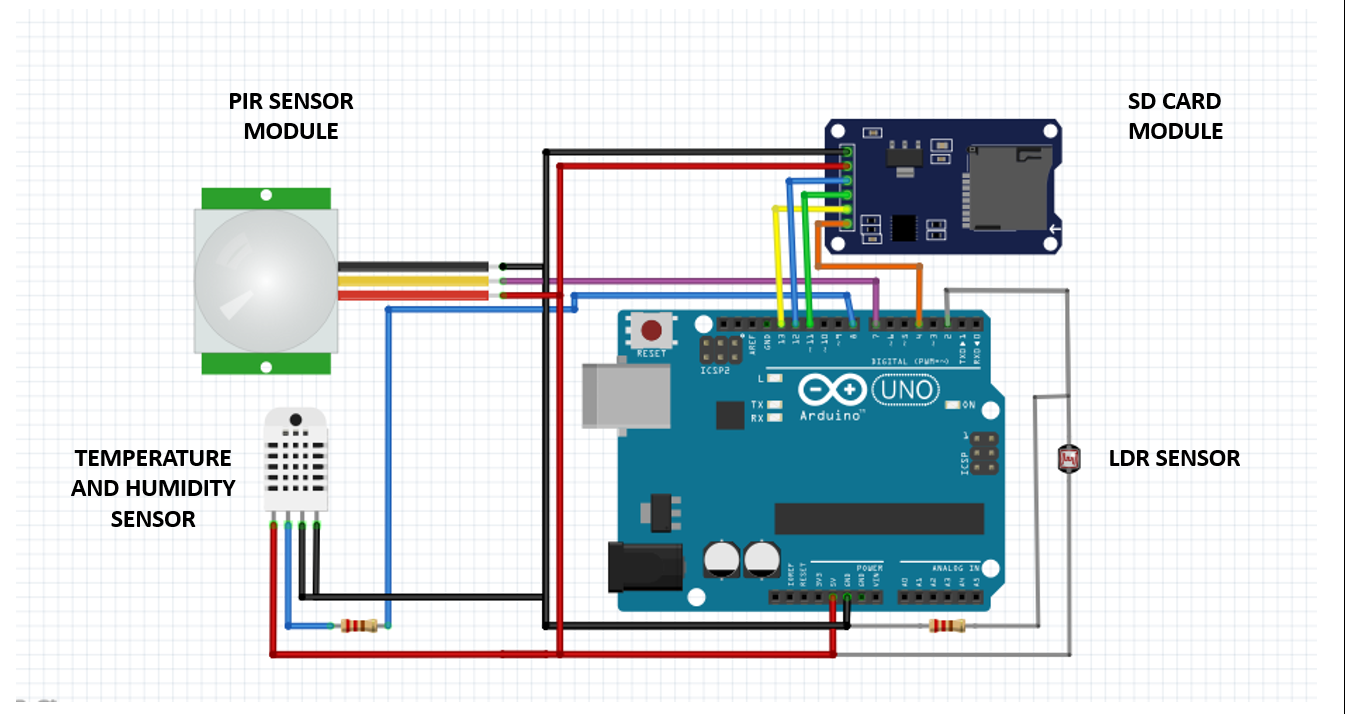


Fig. 4.7. Circuit diagram of the entire circuit

**4.2. Software**

The user interface of our project is the part from which hides the inner implementations of our project, and allows normal people to use it easily. It is a web portal, designed using HTML, CSS templates (Codrops), and Javascript (jQuery, web3.js, node.js).

HTML and CSS is used for the design and for basic functionality, like button clicks redirecting to another webpage, calling javascript functions, displaying retrieved data, entering data, etc. It is basically used for structuring the data.

**4.2.1. The Codrops Framework**

Codrops is a readymade freely available CSS and Javascript framework template which was primarily designed to create more intuitive presentations. We have utilized the CSS templates of this framework in our project, and have also modified those templates a little bit to our liking. [16]

**4.2.2. The Login Page**

The first screen which a person sees is a Login page. Upon entering the username and password, that data is sent for verification to a backend MySql database. If the username and password match, then a message along with the corresponding identifier is sent. The identifier is a single character which specifies that whether the user is a manufacturer, shipper, distributer, retailer, hospital or doctor. Then based on that identifier, the appropriate profile page is shown.

**4.2.3. For the Manufacturer**

For manufacturers, the profile page shows 3 options, namely Sell Medicine, Track Package and Reset Password, along with a Logout button. The Sell Medicine option leads to a page which shows the medicines which have been ordered. They are displayed in the form of a table, with the medicine and its details arranged vertically. The details are medicine name, temperature range (in C), pressure range (in atm) and light intensity (in lux). The Sell button calls the sellArticle() function of the .js file along with the relevant details as parameters. This function then uploads the data to the blockchain.

**4.2.4. For the Shippers, Distributors, Retailers, Hospitals and Doctors**

For shippers, distributors, retailers, hospitals, doctors, etc., the profile page shows 3 options, namely Submit Data, Track Package and Reset Password, along with a Logout button. The Submit Data button calls the sellArticle() function of the .js file, which calls the retrieveData() function, which collects the data recorded by the SmartBox. This data then gets passed up the chain to the sellArticle() function, which uploads it to the blockchain.

**4.2.5. For the Individuals or Guest Users**

For individual customers, they don’t need to login, but can enter as guests by clicking on the Guest button of the Login page. They are then led to the enterData page, where they have to enter the medicine name and the box number, in the format Medicine Name – Batch No. This then leads to the trackTask page, which shows the travel details of that medicine box. The data is shown in the form of a table with columns storing S. No., Location (where it was scanned), Date and Time of scanning, Temperature, Humidity, Light Intensity and PIR status (indicating whether the box was opened prior to the scan or not). The last 4 columns contain information in the form of colours. Red indicating that the limits for that particular parameter had been breached prior to the scan, and green indicating that everything was normal. This acts like a kind of red flag – green flag system.

**4.2.6. The Tracking page**

The Track Package option for all users leads to the enterData page, where they have to enter the medicine name and the box number, in the format Medicine Name – Batch No. This information is then sent to a javascript function which in turn calls the queryChain() function of the smart contract. This function keeps returning data stored in any block which has the same medicine name and batch number as the ones sent as its parameter. This data is then collated and sent to the trackTask page, which shows the travel details of that medicine box, in a table format as mentioned earlier.

**4.2.7. How an Ethereum Contract connects to the Network?**

In general there’s two different types of ways to connect to the ethereum network. There are two different set of technologies to connect to the network. First is used by the developers to connect to the network, this is used to create applications that talk to the network. These applications does so by making the use of the library called Web3. It can be used to send data, money or deploy contracts or essentially whatever we want to develop. Consumers can do so with either of the two.

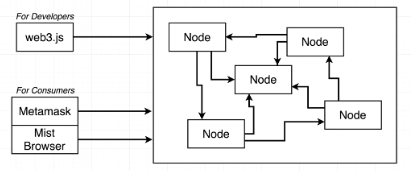


Fig. 4.8. Simplified view of Ethereum nodes

We write the contracts in a contract definition language, as in our case we are using Solidity. The contract that we write needs to be feeded into the solidity compiler. The compiler then splits the compiled code into two different parts. One known as the Byte Code and other part is known as Application Binary Interface (API).

* The first one contains the byte code that is used to actually deploy the code onto the ethereum blockchain on the network.
* The API is really the key for writing applications that can interact with the deployed contracts. As in our case, the Webpage and the Smart Contracts.

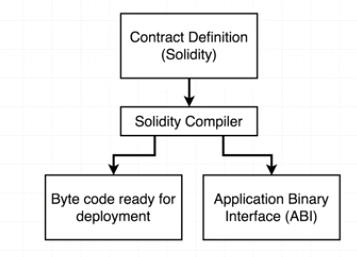


Fig. 4.9. Simplified view of how solidity code is compiled

The bytecode that have been created, contract that we have created goes to the local test ethereum network that we are running on our laptops. This local test network is created by the library called as Ganache/TestRPC. On the other side, we are taking the Application Binary Interface (ABI) that gets fed into the Web3 library which gave use programmatic access to the blockchain.

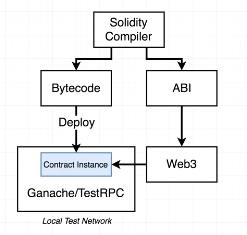


Fig. 4.10. Simplified view of how compiled solidity code is deployed

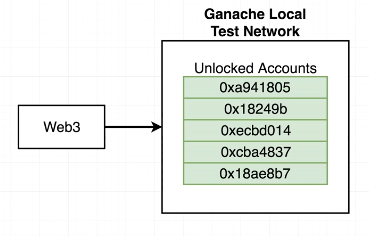


Fig. 4.11. Simplified view of the Ganache local test network

**4.2.7.1. Testing Truffle/Mocha**

Testing is extremely important as slight error in the code can hugely affect the application Truffle is a command line interface for developing applications for the ethereum network. To perform testing through mocha, we can follow the same cycle given below again and again. This involves deploying the code onto the local network, manipulating the values of the contract, then make assertions about the outputs or values that it takes and finally decide if it is feasible or not.

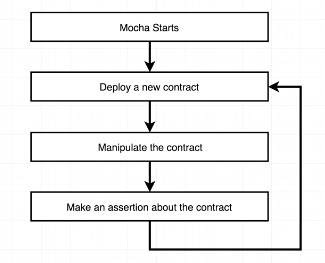


Fig. 4.12. Simplified view of Mocha testing

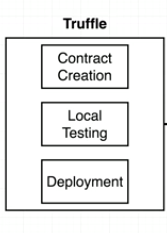


Fig. 4.13. Simplified view of Truffle testing

**4.2.7.2. Starting the application**

To start the application, we first start Ganache, which provides us with some virtual accounts, each containing 100 ethers to work with.

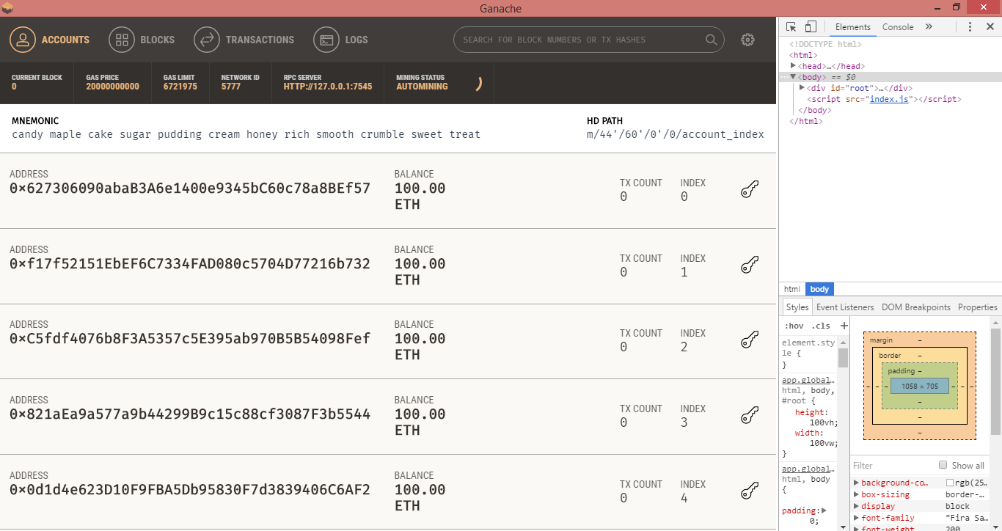


Fig. 4.14. Ganache showing accounts with full ether

We then open Windows PowerShell, and activate truffle and migrate our smart contracts to the network setup up by Ganache. We then turn on the lite server to host our application.

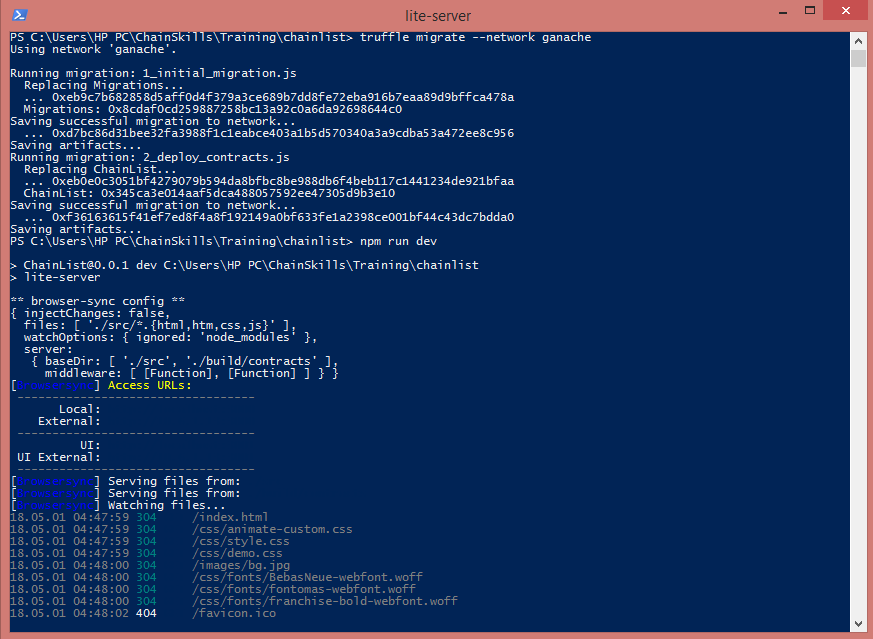


Fig. 4.15. Activating truffle and lite server

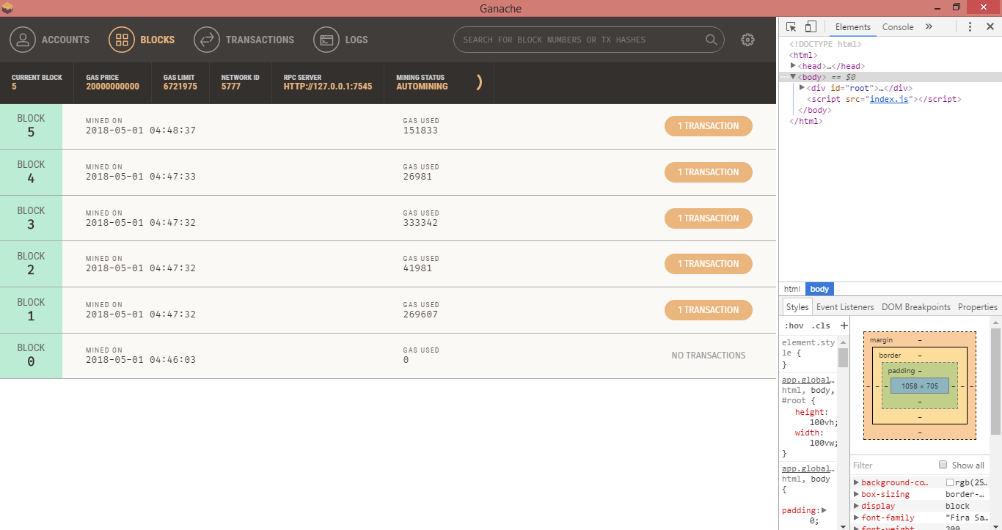


Fig. 4.16. New blocks mined in ganache due to selling medicine

**5. CONCLUSION**

Blockchain technology, with its de-centralised structure, immutable nature and robust architecture (utilizing complex consensus algorithms, proof of work, and recently proof of stake requirements, computation intensive mining processes), is increasingly becoming the go-to technological option for services which require high levels of security and trust of consumers, like banking, enterprise grade cloud storage and remote working facilities, legal data, medical data, etc. Our project attempts to solve a major problem plaguing the medical field, especially the pharmaceuticals industry, i.e. the problem of counterfeit and substandard medicines flooding the market. Such medicines often contain less than permissible levels of the active ingredient, and sometimes no ingredient at all. In extreme cases, they might contain other chemicals which are harmful for human consumption.

Our application tracks the travel history of a box of medicine, including its travelling conditions (temperature, humidity, light exposure). It can also detect any unauthorised opening of the medicine box. This will ensure that any authorised person in the supply chain will be able to detect if the box of medicine has been exposed to any physical condition which might reduce its efficacy, or if any suspicious activity has occurred with the box of medicine, including the location where such activity had occurred. They can then take appropriate actions, like rejecting the medicine box, informing the manufacturer or the organisation where the red flag was raised, inspecting the box themselves, etc.

This is not a new concept, and some other organisations are also working on similar concepts, like the MediLedger Project, where also blockchain is being used to track-and-trace prescription medicines. They are also allowing full privacy, non-leakage of business intelligence and capability of drug verification. But they don’t maintain authenticity during the entire supply chain, and they also do not apply any proof of work to validate and verify a transaction, which we do. Even IBM is working on a similar project in Kenya, where they are utilizing smartphone based QR code scanners to authenticate the identity of each party in the supply chain. But they are not tracking the physical conditions to which the medicine might be exposed, nor any tampering done to the medicine box, which we are doing using our Smart Box.

We hope that our application will be able to make a positive difference in the fight against the scourge of counterfeit medicines.

**6. FUTURE WORK**

Our application has a lot of potential to be developed further into a full-fledged platform, with an ethereum blockchain forming its backbone. There are several features which we haven’t incorporated as of yet because of lack of time and resources. We believe that these features can be incorporated in the future and they will add great value to the application. Some of the ideas that we have regarding the features are listed below.

**Blockchain based login and registration system:** The login system, comprising of a username and password, can be enabled using blockchain, from the current system of a centralised database containing all the usernames, passwords and identifiers. Registration of new members can also be made blockchain-based, once the government authorities fully embrace this technology, as there are various legal provisions involved in the medical industry.

**Blockchain based E-commerce platform:** We can evolve this application into an e-commerce platform, which utilises an ethereum blockchain to verify all transactions, which includes placing orders, accepting orders, order tracking, which includes tracking physical conditions of medicine box (temperature, humidity, light intensity) and tracking any unauthorised access to the box, and raising the appropriate red flags. Verification and security of payments can also be ensured using blockchain.

**Implementation of realtime location tracking capability:** The relevant stakeholders will be able to track the actual location of the Smart Box throughout the delivery route. This would be made possible by implementing GPS support.

**Expansion in Scope of Items that can be delivered:** It encompasses the all the goods and products which require specific environmental parameters and/or conditions to be maintained throughout the entire duration the delivery, such as live plants, volatile materials, chemicals and substances. Also various high value commodities which are prone to theft and undesired tampering can also be shipped using our implementation.

**Smart Containers:** This idea involves evolving our product from Smart Box to a Smart Container which would be able to regulate the temperature and humidity levels within the allowed range of the drugs that are being transported.

**7. REFERENCES**

[1] Y. Sompolinsky and A. Zohar, “Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains” IACR Cryptology ePrint Archive, 2013

[2] Nakamoto Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf

[3] Gavin Wood “Ethereum: A Secure Decentralised Generalised Transaction Ledger”, EIP-150 Revision; gavwood.com/paper.pdf

[4] G Zyskind, O Nathan, A. Pentland, “Decentralizing Privacy: Using Blockchain To Protect Personal Data,”Security and Privacy Workshops (SPW), 2015 IEEE, May 2015

[5] J. Spasovski and P. Eklund “Proof of Stake Blockchain: Performance and Scalability for Groupware Communications” The 9th International Conference on Management of Digital EcoSystems 2017

[6] K. Christidis and Michael Devetsikiotis “Blockchains and Smart Contracts for the Internet of Things” IEEE Acess, Volume 4

[7] Ali Dorri, Salil S.Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions”

[8] A. Kiayias, A. Russell, B. David, R. Oliynykov. “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol”

[9] A. Fahad Abdulaziz Alghannam, Z. Aslanpour, S. Evans, F. Schifano, “A systematic review of counterfeit and substandard medicines in field quality surveys” Integrated Pharmacy Research and Practice 2014.

[10] J. Kuanpoth “Combatting counterfeit drugs: Case studies of Cambodia, Vietnam and Thailand” (2017) 13 Journal of Generic Medicines: The Business Journal of Generic Medicines Sector 1-16.

[11] V. Li and S. Webb, “A bitter pill to swallow: the problem of, and solutions to, Sub-Saharan Africa’s counterfeit pharmaceutical trade”

[12] <http://chainskills.com/2016/11/21/what-qualifies-as-a-blockchain/>

[13] <https://www.weforum.org/agenda/2015/08/how-do-we-combat-the-problem-of-counterfeit-drugs/>

[14] <https://www.npr.org/sections/goatsandsoda/2017/11/29/567229552/bad-drugs-are-a-major-global-problem-who-reports>

[15] E. A. Blackstone, J. P. Fuhr Jr., S. Pociask, “The Health and Economic Effects of Counterfeit Drugs”, Am Health Drug Benefits, Vol. 7, Ver. 4, June 2014

[16] <https://github.com/codrops>

[17] <https://coincentral.com/what-is-ethereum/>

[18] <https://www.edureka.co/blockchain-tutorial/>

[19] <https://www.ethereum.org/>

[20] <https://blockgeeks.com/guides/smart-contracts/>

[21] <https://www.ethereum.org/>ether

[22] <https://blockgeeks.com/guides/dapps/>

[23] <https://coinsutra.com/private-blockchain-public-blockchain/>

[24] [https://www.arduino.cc/en/Guide](https://www.arduino.cc/en/Guide%20)

[25] <https://www.edureka.co/blog/blockchain-tutorial/>

[26] <https://github.com/jbeynon/sdfatlib>

[27] <https://www.arduino.cc/en/Reference/SPI>

[28] <https://www.instructables.com/technology/arduino/>

[29] <https://www.arduino.cc/en/Guide/Introduction>

[30] <https://www.tutorialspoint.com/arduino/index.htm>

[31] <https://www.arduino.cc/en/Guide>

[32] <https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor?view=all>

[33]https://www.edureka.co/blog/blockchain-tutorial/

[34] <https://blockgeeks.com/guides/ethereum/>

[35] <https://blockgeeks.com/guides/ethereum/>