Blockchain In Retail

A PROJECT REPORT

submitted by

SHREEJIT VERMA (14BCE0728)

in partial fulfillment for the award of the degree of

B. Tech

in

Computer Science and Engineering

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Vellore-632014, Tamil Nadu, India

School of Computer Science and Engineering

APRIL, 2018

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

DECLARATION

I henceforth declare this project entitled **"Blockchain In Retail"** submitted by Shreejit Verma to the School of Computer Science and Engineering, Vellore Institute of Technology, Vellore-14 towards the partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out by me under the supervision of **Prof. Vijayarajan V, Assistant Professor.** I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma of this institute or of any other institute or university.

Signature

Name : Shreejit Verma

Reg.No: 14BCE0728

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

CERTIFICATE

The project report entitled "**Blockchain In Retail**" is prepared and submitted by **Shreejit Verma (Register No: 14BCE0728),** has been found ground-breaking and immensely valuable in terms of scope, quality and presentation as partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** in Vellore Institute of Technology, Vellore-14, India.

Guide
(Name & Signature)

Internal Examiner
(Name & Signature)

External Examiner
(Name & Signature)

ACKNOWLEDGEMENT

I wish to express my heartfelt gratitude and thanks to my respected guide **Prof. Vijayarajan V (**Associate Professor at the School of Computer Science and Engineering) who helped me with his valuable suggestions throughout the project. He was my mentor and my guide throughout my project. Without his assistance and guidance, I could not have completed the project within the specified time.

I express my sincere gratitude and thanks to **Prof V. Santhi, Head of Department (HOD), SCOPE** for the confidence she had in us throughout the project. I will always remain grateful to her for her support, guidance and encouragement throughout the project.

I am also very thankful to the **Dr. R. Saravanan DEAN, SCOPE** for giving us the required technical support throughout the project and allowed us to utilize all the resources required for the completion of the project and guidance at each and every step throughout the project.

At last, I would like to express my sincere gratitude to my college **Vellore Institute of Technology** for providing me an opportunity to undertake and complete such an interesting project.

Place: Vellore

Date:

Name of the student

Shreejit Verma
14BCE0728

CONTENTS

4.2.1.5. Domain Requirements

4.2.1.6. User Requirements

4.2.2. Non-Functional Requirements

4.2.2.1. Product Requirements

4.2.2.1.1. Efficiency (in terms of Time and Space)

4.2.2.1.2. Reliability

4.2.2.1.3. Portability

4.2.2.1.4. Usability

4.2.3. Engineering Standard Requirements

- Economic
- Environmental
- Social
- Political
- Ethical
- Health and Safety
- Sustainability
- Legality
- Inspect ability

4.2.4. System Requirements

4.2.4.1. H/W Requirements

4.2.4.2. S/W Requirements

5. Results and Discussions

5.1. Sample Test Cases

5.2. Summary of the Result

6. Conclusion, Limitations and Scope for future Work

Appendix

Annexure – I

References

LIST OF TABLES

Title **Page No.**

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Expansion
P2P	Peer-to-peer
GETH	Go Ethereum
API	Application Program Interface
PHP	Hypertext Preprocessor
IDE	Integrated development Environment
Gas	Cost of Opcode computational sum in Ethereum.
web3j	(Web3 Java Ethereum Đapp API)

ABSTRACT

Consumer trust is a big issue right now, especially when more consumers seek goods that are premium, unique, locally sourced, and/or humane. But until now, there's been little consumers could do to truly verify the quality of their purchases. As retailers struggle to make the purchase secure, transparent and do more with less in a margin-squeezed environment, the potential for Blockchain to establish trust and reduce operating costs has been in great demand. Aim of this project is to make retail free from intermediaries (e.g. distributors, whole sellers, marketing companies) and make retail trustworthy, less costly and easily accessible for people. The retail market has many entities who charge some money for selling of a product. Offline market is struggling to compete with e-commerce websites. Consumer has to pay much more than the actual price of the product because of the intermediate entities involved in the process of retail, also offline market doesn't have that good of management, security and workflow than e-commerce websites. It is becoming very tough for a normal manufacturer or seller to sell his/her product because of less exposure to the market and the competitive pricing. Also There is no standard currency for buying products; the conversion of money and the trade policies across the border adds with the product price and make it costly and thus attracting very small market. For solving these problems Blockchain is used as a retail platform. It helps in streamline operations, ensure product authenticity, enable tighter supply chain collaboration, remove the intermediate cost, make the process transparent, secure and easily accessible to everyone. Smart contracts are used with only append ledger accessible to everyone which reduces chances of fraud and better record management. Ethereum (cryptocurrency) is used as standard way to transfer funds which cut the cost of currency conversion and standardizes the process for everyone.

Key Words: Bitcoin, Blockchain, Cryptocurrency, Ethereum, Hash, Loyalty, Retail, Geth, Ganache, Truffle, Metamask, Solidity, web3.

INTRODUCTION

1. Introduction

1.1. Theoretical Background

Blockchain is an emerging technology for decentralization of applications and transactional data sharing across a large network of untrusted participants. It enables new forms of distributed software architectures. Although the technology was mainly adopted in digital currency in initial days, but it is a promising technology for other areas too. Blockchain technology can be used in some business processes in the retail sector to benefit the customers and the retailers to a great extent.

Blockchain networks create proof of ownership by using unique digital signatures that rely on both public encryption keys known to everyone on the network and private keys known only to the owner. Blockchain platforms can be public (i.e. permission less), like Bitcoin, with anyone allowed to submit a transaction and take part in validating other transactions. Or they can be private (i.e., permissioned), where only authorized participants can share and validate transactions in the network. This allows for innovations that address the speed, privacy and scalability concerns of public Blockchain while reinforcing the validity of transactions.

For retailers, Blockchain holds the promise of delivering trust in a product, transaction or the integrity of data more effectively and at lower cost than ever before. Blockchain applications could help retailers improve supply chain visibility, ensure product provenance and authenticity, speed up transactions, reduce processing fees, and improve the management of networked loyalty programs.

Blockchain is a distributed ledger technology that underlies cryptocurrencies like Bitcoin. It provides a way to record and transfer data that is transparent, safe, auditable, and resistant to outages. The Blockchain has the ability to make the organizations that use it transparent, democratic, decentralized, efficient, and secure. It's a technology that holds a lot of promise for the future, and it is already disrupting many industries.

A Blockchain protocol operates on top of the Internet, on a P2P Network of computers that all run the protocol and hold an identical copy of the ledger of transactions, enabling P2P value transactions without a middleman though machine consensus. Blockchain itself a file – a shared and public ledger of transactions that records all transactions from the genesis block (first block) until today. The ledger is built using a linked list, or chain of blocks, where each block contains a certain number of transactions that were validated by the network in a given timespan. The crypto-economic rulesets of the Blockchain protocol (consensus layer) regulate the behavioral rulesets and incentive mechanism of all stakeholders in the network.

The game theory is used to generate or mine each block using consensus algorithm like 'proof-of-stake' or 'proof-of-work' algorithm. The cryptographic rules define the difficulty of mining and reward for mining.

This ledger runs on a peer-to-peer (P2P) network of computers. Distributed consensus based on economic incentive mechanisms (game theory) combined with cryptography allows for secure P2P validation of transactions, thus bypassing the need for traditional trusted third parties.

1.2. Motivation

Earlier Blockchain was developed for transactions of money only. In recent years, it was proved that it could be used for any kind of peer to peer value transaction over Internet. The concept of programmable contracts was introduced by Ethereum project. It separated the Blockchain layer from the contract layer. The ledger itself could be programmed using languages like Solidity to perform some logical processing for transactions. This opened total new opportunities for creating smart contracts for any transaction with trust and transparency over Internet.

The snippet of code which works based on Blockchain network is called smart contract. It is where the assets are controlled digitally by implementing logic inside the code implementing satisfying rule and performs some steps. This provides a suitable environment for renting contract agreement and creation. The renting could be done easily with less manual intervention and with trust and transparency with very low rate of possible fraud.

Blockchain could help retailers address a variety of pressing business issues, including the following:

- **Ensuring product authenticity**. Tracking provenance. Grocery retailers specializing in organic and GMO-free food products would ben- e t from the ability to shore up confidence among consumers suspicious that organic labels are just a marketing tool and strategy to charge higher prices. Supermarket chains and their supply chain partners could deploy a Blockchain solution to raise confidence in their products by allowing customers to track the journey of a product from the farm to the store.

  The proliferation of forgeries that are difficult to identify can result in declining sales and a deterioration in the value of genuine products for designers of luxury consumer goods. A Blockchain solution can renew trust by allowing customers to scan a code permanently etched into the product and access the entire history of the product, including the chain of ownership.

  Enhancing customer loyalty/rewards programs. More than $400 billion in consumer loyalty rewards are issued by businesses all across the world each year, and many companies today have expanded their programs to cover multiple brands in an effort to increase customer loyalty programs they are enrolled in, and many of the loyalty points created each year go unused, resulting in balance sheet liabilities. A Blockchain application would allow users to easily redeem points across different merchants and platforms (e.g., iOS, Android and web), improving customer satisfaction and reducing liabilities, while also cutting operating costs and decreasing the potential for fraud.

  Many of these examples will pivot on Internet of Things' (IoT) sensors and related instrumentation to bump Blockchain from its infrastructure roots into a catalyst for Genesis of Things, which marries Blockchain's shared infrastructure with 3-D printing,

exemplify how this emerging technology can elevate trust and introduce new market opportunities for manufacturers, logistics companies and retailers across the value chain

- **Improving inventory management**. With the shorter product life cycles and increasing complexity of Supply chain management, sales forecasting has become more difficult for national fashion apparel retailers. These retailers and their supply chain partners could implement a Blockchain solution that provides a single source of truth and uses smart contracts to enable the automatic execution of payments and orders. The improved supply chain visibility would increase operating efficiency and allow more accurate forecasts, preventing over-ordering and minimizing lost sales due to understocking and overstocking.

1.3. Aim of the proposed Work

The process of a retail transaction comes with high costs of intermediate cost, transaction and searching, therefore making it inefficient and time-consuming. Due to these inefficiencies, barriers exist, which hinder various entities to enter the market. Existing platforms are somewhat difficult, as people bump into all kinds of problems, when trying to identify their optimal object. Rules, conditions and fees are dictated to users.

Our project pursuits the vision that listing data and managing information about the transactions in Retail markets should be a free service. Anyone should be able to simply list an object without needing permission to do so. By being built on Ethereum, our proposed system will be able to provide this model of open and free access to network participants. Users data cannot be accessed by anyone else, while third party advertisements, like competing brokers, are effectively prevented.

1.4. Objective(s) of the proposed work

The objective of project:

- Deploying smart contract over Blockchain technology like Ethereum.
- Smart contract will be implemented using Solidity language
- Build a decentralized application for better management of Retail Services.

- Develop remote client application to allow people for easy access and perform transactions on using smart contract over the Blockchain.
- Creation of Retail Website which provides people all across the world to buy and sell products without involving any intermediaries.
- Providing Ethereum crypto-currency for money transfer thus cutting the currency conversion fees and cross border trade policies.

2. Literature Survey

2.1. Survey of the Existing Models/Work

This white paper [1] explores how the bold and state-of-the-art use of Blockchain can help retailers drive counterfeit goods from the marketplace, reduce time-consuming transaction payments, improve operating efficiencies, slash the cost of proving product claims and strengthen customer relationships. Retailers face a myriad of steep macroeconomic challenges, from global competition and the growth of online shopping, to margin pressure – and that's just the beginning. On a micro level, retailers contend with:

- **Empowered consumers**, who simultaneously demand both lower prices and higher quality.
- **Heightened demand for product authenticity**. Discerning customers increasingly want proof that their diamonds are conflict- free and their vegetables were grown on an organic farm, not just slapped with an organic label.
- **Higher costs from third-party payment processors**, many of which demand ever-higher transaction fees.
- **Pressure from counterfeiters**, who steal sales (and undermine the legitimacy of luxury brands) by flooding the market with fakes that appear virtually indistinguishable from the real thing.

This [2] paper focuses on the fact that Blockchain technology is poised to fundamentally alter the retail industry. Yet, many retailers have not taken the steps necessary to understand how the technology can help their business and what will be required to

embrace blockchain thinking and technology. Retailers should begin collaborating with external stakeholders and partners on joint projects to stress-test how and where Blockchain's distributed ledger and shared infrastructure, in combination with smart contracts, can fit into their businesses. Retailers that move aggressively will enjoy an early advantage by converting analog and labor-intensive tasks into digitally-automated processes.

This [3] paper focuses on the fact that Today's retail customers are highly concerned about fair trade practices, and the truth about the claims that retailers make about their merchandise. Empowered by social media, the new age omnichannel customer is conscious, more informed and demands authentic and ethically sourced products than ever before. This leaves retailers with no choice but to improve their visibility into the movement of produce from farm-to-fork or products from factory-to-home. Additionally, retailers stand to gain significant operational advantages with these enhanced visibility initiatives.

This [4] paper has discussed about the blockchain technology along with some of its significant features and benefits. The technology is still evolving with a lot of scope for different domains and industries and is set to change the world. But it is not free from challenges; some of them have been highlighted too. Although blockchain is the technology behind Bitcoin, but its use is not limited to financial domain only. Retail industry will start reaping the benefits of blockchain through improved transparency of products, more efficient supply chain management, better loyalty management system, improved customer profiling, fight against counterfeiting etc. leading to increased customer satisfaction and higher profit margin for retailers. The year 2016 revealed blockchain as more disruptive technology to the retail industry than any other industry, and in 2017 blockchain is gradually becoming the dominant hype phrase for retailing.

This [5] paper has discussed about smart contracts. Smart contracts is an appealing feature of blockchain technology is A smart contract is executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party. In this paper, we conduct a

systematic mapping study to collect all research that is relevant to smart contracts from a technical perspective. The aim of doing so is to identify current research topics and open challenges for future studies in smart contract research. We extract 24 papers from different scientific databases. The results show that about two thirds of the papers focus on identifying and tackling smart contract issues. Four key issues are identified, namely, codifying, security, privacy and performance issues. The rest of the papers focuses on smart contract applications or other smart contract related topics. Research gaps that need to be addressed in future studies are provided.

Traditional retailers face a challenging business environment, marked by continuing margin pressure, encroaching efforts of digital-native rivals and greater global competition. At the same time, they must contend with issues such as limited supply chain visibility, empowered consumers, high transaction fees and the need to battle counterfeit products.

As retailers struggle to do more with less in a margin-squeezed environment, the potential for Blockchain to reduce operating costs is one of its principal attractions

For retailers, Blockchain holds the promise of delivering trust in a product, transaction or the integrity of data more effectively and at lower cost than ever before. Blockchain applications could help retailers improve supply chain visibility, ensure product provenance and authenticity, speed up transactions, reduce processing fees, and improve the management of networked loyalty programs.

2.2. Summary/Gaps identified in the Survey

Retailers face a myriad of steep macroeconomic challenges, from global competition and the growth of online shopping, to margin pressure – and that's just the beginning. On a micro level, retailers contend with:

• **Empowered consumers,** who simultaneously demand both lower prices and higher quality.

• **Heightened demand for product authenticity**. Discerning customers increasingly want proof that their diamonds are conflict-free and their vegetables were grown on an organic farm, not just slapped with an organic label.

• **Pressure from counterfeiters**, who steal sales (and undermine the legitimacy of luxury brands) by oohing the market with fakes that appear virtually indistinguishable from the real thing. **Higher costs from third-party payment processors**, many of which demand ever-higher transaction fees.

•**Closing the talent gap** Retailers face challenges in securing Blockchain talent, So far, 42% of respondents said their organization has assessed the internal skills/talent requirements to support a Blockchain initiative, although 50% said that such an assessment is in progress and 39% of respondents consider procuring talent and expertise to be one of the top internal barriers to its adoption.

Retail organizations are using a mix of internal and external strategies to close the talent gap. The most common internal strategies for obtaining needed Blockchain skills were innovation labs (56%), training (such as attending technical workshops) (49%) and hiring new workers (43%) (see Figure 6, next page). But retailers are also using a variety of external strategies to acquire additional expertise, including partnerships with Blockchain technology companies (47%), targeted acquisitions (40%) and investing in start-ups (36%).

Many respondents acknowledged that their organization will need additional Blockchain expertise in a variety of areas, including risk management (58%), compliance (56%), cybersecurity (54%), legal (56%), and business strategy (49%). However, we believe that many respondents are underestimating the additional Blockchain expertise that will be required. This is especially the case in the area of technical skills, where only 37% of respondents believed their organization will need additional expertise. This is especially the case in the area of technical skills, where only 37% of respondents believed their

organization will need additional expertise. In our experience, most retail organizations will discover that they need more expertise in Blockchain specific areas such as PKI infrastructure, information architecture, software engineering, network infrastructure and integration, and user interface/user experience, among others.

Blockchain can help retailers overcome these challenges and more. It can do so by providing low-cost immutable trust at every step of the value chain, from product design and chain of custody through transactional information. While Blockchain pioneers will face challenges, retailers that turn a blind eye to this emerging opportunity are at risk of missing early-mover advantage and contributing to the restructuring of the retail industry.

3. Overview of the Proposed System:

3.1. Introduction and Related Concepts

The Blockchain for creating smart contract and usage of web client simplifies the process of Retail. The Blockchain is a distributed ledger using peer to peer network and computation to perform and record transactions. The batches of valid transactions are stored on blocks and Merkle tree is generated by encoding and hashing these blocks. The previous block's cryptographic hash is included in the current block in the Blockchain. This links them together forming a chain. This provided integrity and way to confirm validity of the adjacent blocks. We could confirm it iteratively by moving backwards until we reach the first or genesis block. The peer to peer networking allows nodes to communicate with other nodes.

The new block is generated by performing 'proof-of-work' which uses high computation process to generate a 'nonce'. This 'nonce' should satisfy the conditions and its computation difficulty depends on the problem on which all nodes on network are working. It helps in order to reach consensus among other nodes and node mining block. The creator is rewarded for mining new block. The Ethereum is such a Blockchain system based on these concepts. The Ethereum also supports smart contract which can be programmed as per requirement.

3.2. Framework, Architecture or Module for the Proposed System:

The architecture of the project consist of Blockchain to store transaction, web client for interacting with the Blockchain to perform transactions and database to save some information about users.

The user communicates through the client application with block chain.

The application consists of following modules:

1. Smart contract: Contains all logical information and function to process the transactions. The contract is programmed using “Solidity language”. The contract logic is implemented using high level language called solidity and is deployed on Ehthereum Blockhain.

2. Go Ethereum API: It is application which is used to create Blockchain. It can be used for mining and also to interact with Blockchain. It runs on multiple computers and act as distributed ledger. The contract is deployed using API and validated by using API provided by GO Ethereum

3. Ganache: It is a personal blockchain for Ethereum development you can use to deploy contracts, develop your applications, and run tests. It lets you see what's happening under the hood during development, and lets you introspect blocks and transactions to better understand how your application behaves.

4. Metamask: It is an extension for Chrome or Firefox that connects to an Ethereum network without running a full node on the browser's machine. It is the easiest way to interact with dapps in a browser. It can connect to the main Ethereum network, any of the testnets (Ropsten, Kovan, and Rinkeby), or a local blockchain such as the one created by Ganache or Truffle Develop.

5.web3j (Web3 Java Ethereum Đapp API) : web3j is a lightweight, highly modular, reactive, type safe Java and Android library for working with Smart Contracts and integrating with clients (nodes) on the Ethereum network.

Features:

- Connecting to a node on the Ethereum network
- Reading a value from the deployed smart contract
- Updating a value in the deployed smart contract
- Loading an Ethereum wallet file
- Sending Ether from one address to another
- Deploying a smart contract to the network
- Viewing an event logged by the smart contract

6. Solidity: Solidity is a contract-oriented, high-level language for implementing smart contracts. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

7.. Truffle: Truffle is a development environment, testing framework and asset pipeline for Ethereum, aiming to make life as an Ethereum developer easier. With Truffle, you get:

- Network management for deploying to many public & private networks.
- Interactive console for direct contract communication.
- Instant rebuilding of assets during development.
- External script runner that executes scripts within a Truffle environment.
- Built-in smart contract compilation, linking, deployment and binary management.
- Automated contract testing with Mocha and Chai.
- Configurable build pipeline with support for custom build processes.
- Scriptable deployment & migrations framework.

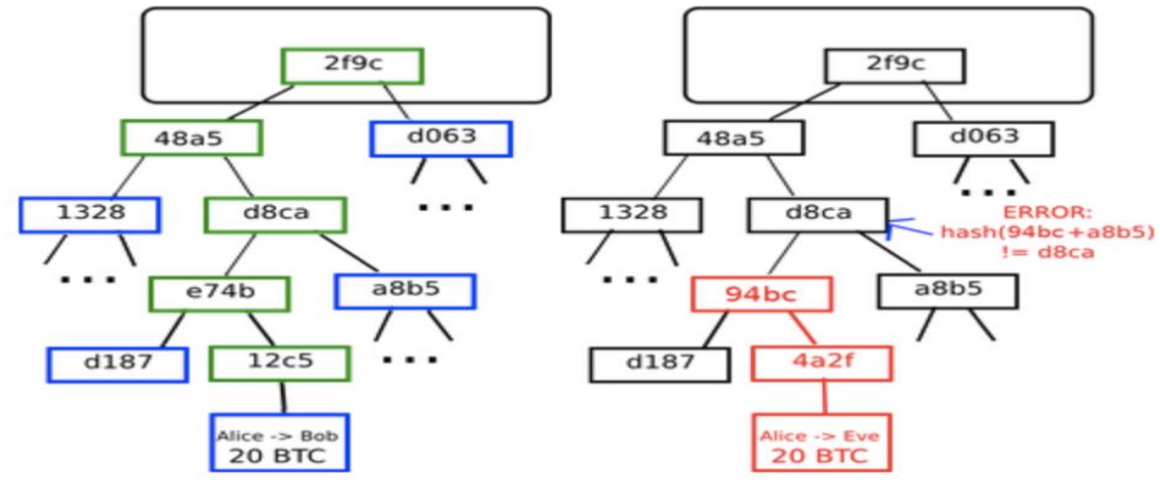

Fig 1: Merkle Tree Diagram

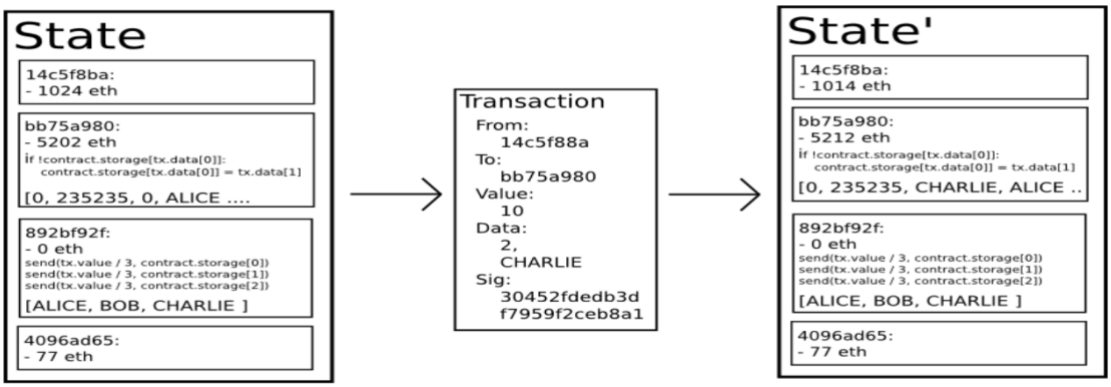

Fig 2: Transaction State Diagram

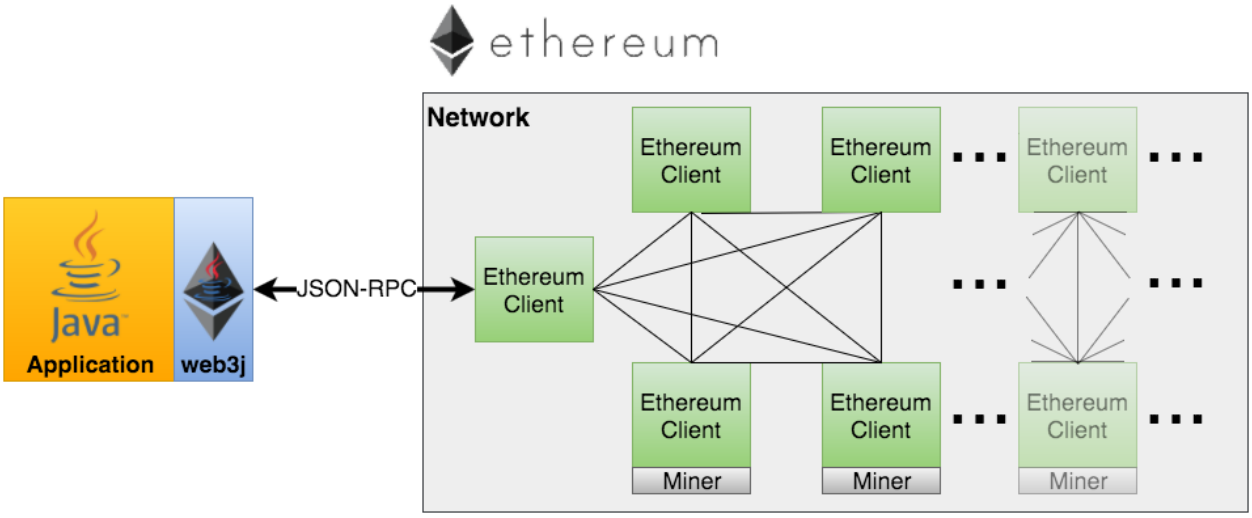

Fig 3: Blockchain Network of Nodes

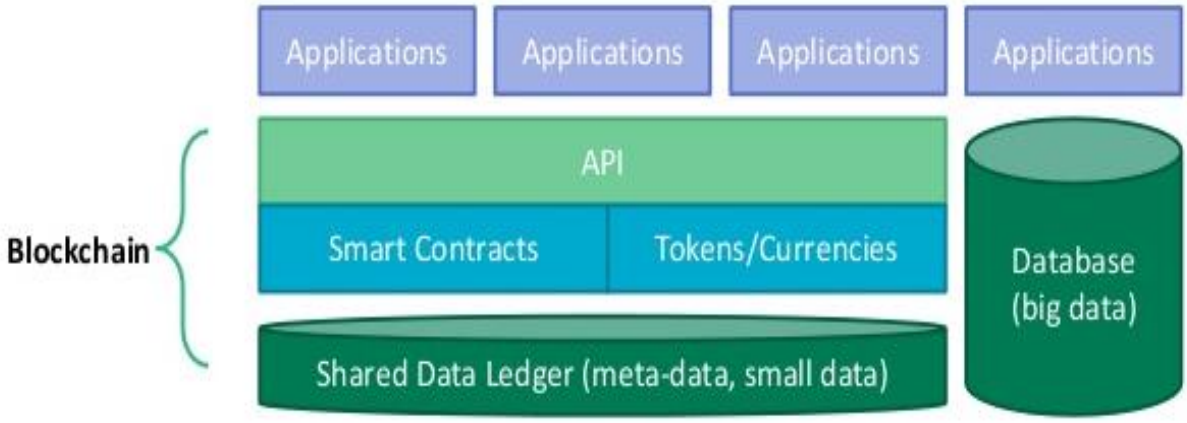

Fig 4: Architecture of Application

3.3. Proposed System Mode

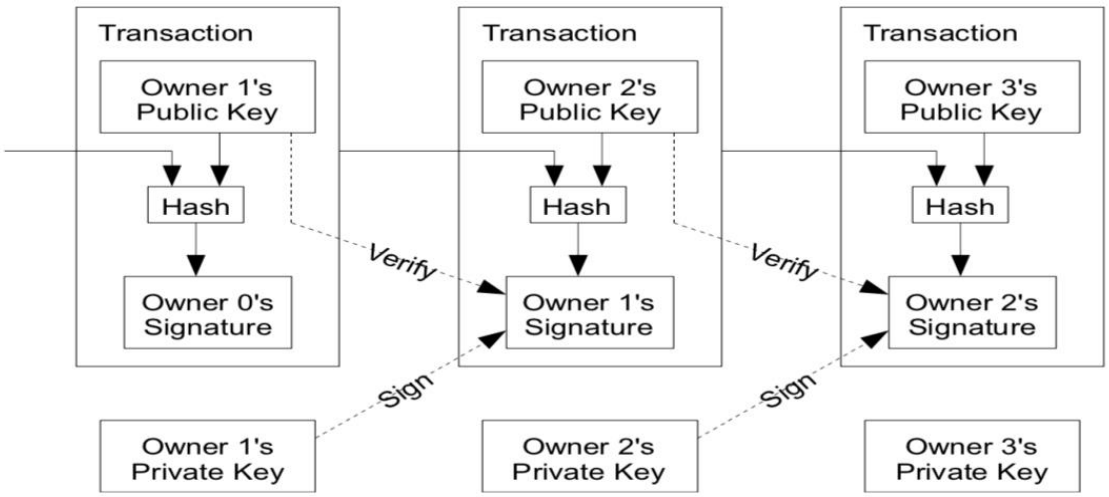

Fig 5: Evaluation of Transaction (Addition of Blocks)

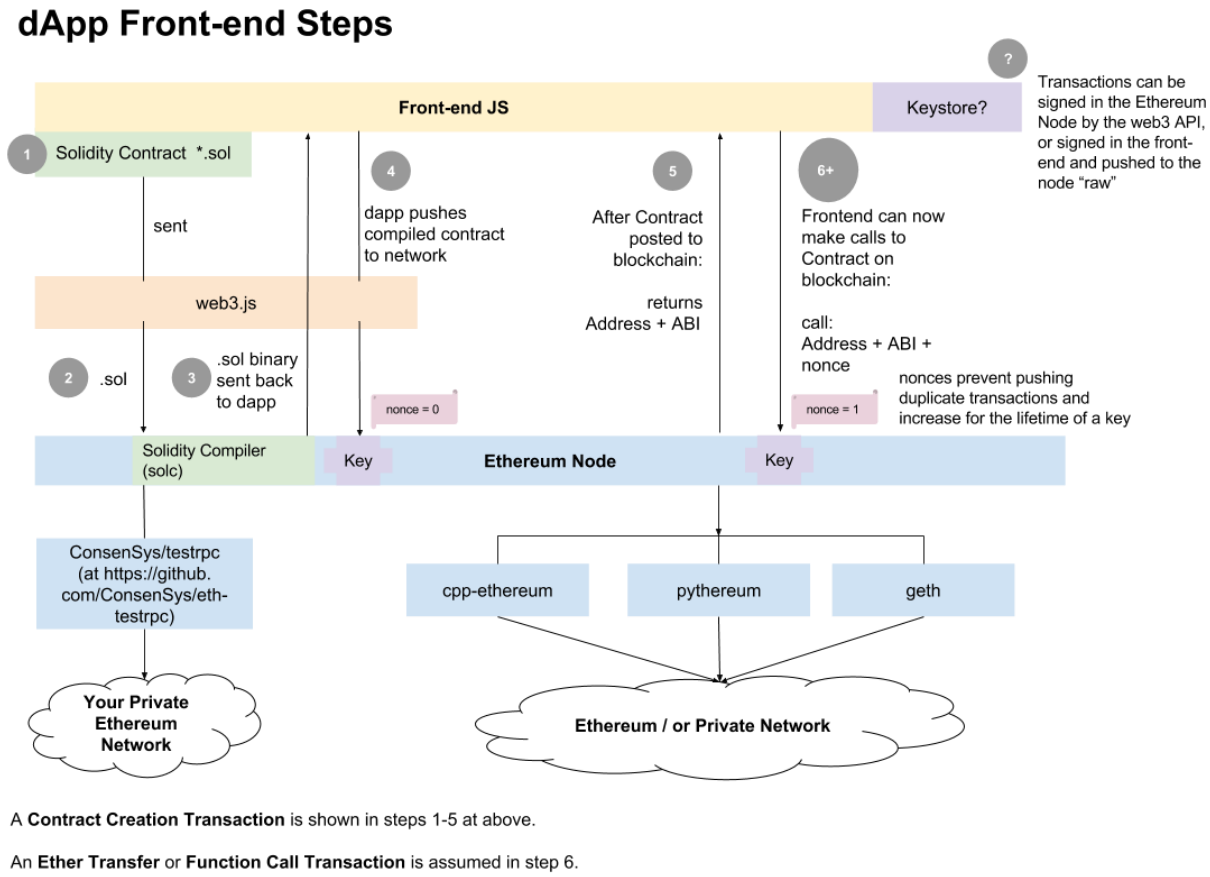

Fig 6: System Architecture of Application

Steps to Deploy a Smart contract:

- Truffle init in specific directory
- Write a contact in contract directory
- Add the contract name to “contracts”in config/app.json
- Start the ethereum node
- Truffle deploy

Workflow for Deploying Smart Contracts

The workflow is:

1. Start an **Ethereum node** (e.g. geth or testrpc or ethersim)
2. **Compile** your Solidity smart contract using solc => get back the binary
3. **Deploy** your compiled contract to the network. (This step costs ether and signs the contract using your node’s default wallet address, or you can specify another address.) => get back the contract’s Blockchain address and ABI (a JSON-ified representation of your compiled contract’s variables, events and methods that you can call)
4. **Call** stuff in the contract using web3.js’s JavaScript API to interact with it (This step may cost ether depending on the type of invocation.)

Contract Class:

```
pragma solidity ^0.4.18;

import "./Ownable.sol";

contract ChainList is Ownable {

  // custom types
```

```
struct Article {
  uint id;
  address seller;
  address buyer;
  string name;
  string description;
  uint256 price;
}
// state variables
mapping (uint => Article) public articles;
uint articleCounter;
// events
event LogSellArticle(
  uint indexed _id,
  address indexed _seller,
  string _name,
  uint256 _price
);
event LogBuyArticle(
```

```
  uint indexed _id,
  address indexed _seller,
  address indexed _buyer,
  string _name,
  uint256 _price
);
// deactivate the contract
function kill() public onlyOwner {
  selfdestruct(owner);
}
// sell an article
function sellArticle(string _name, string _description, uint256 _price) public {
  // a new article
  articleCounter++;
  // store this article
  articles[articleCounter] = Article(
    articleCounter,
    msg.sender,
    0x0,
```

```
    _name,
    _description,
    _price
  );
  LogSellArticle(articleCounter, msg.sender, _name, _price);
}
// fetch the number of articles in the contract
function getNumberOfArticles() public view returns (uint) {
  return articleCounter;
}
// fetch and return all article IDs for articles still for sale
function getArticlesForSale() public view returns (uint[]) {
  // prepare output array
  uint[] memory articleIds = new uint[](articleCounter);
  uint numberOfArticlesForSale = 0;
  // iterate over articles
  for(uint i = 1; i <= articleCounter;  i++) {
    // keep the ID if the article is still for sale
    if(articles[i].buyer == 0x0) {
```

```
      articleIds[numberOfArticlesForSale] = articles[i].id;
      numberOfArticlesForSale++;
    }
  }
  // copy the articleIds array into a smaller forSale array
  uint[] memory forSale = new uint[](numberOfArticlesForSale);
  for(uint j = 0; j < numberOfArticlesForSale; j++) {
    forSale[j] = articleIds[j];
  }
  return forSale;
}
// buy an article
function buyArticle(uint _id) payable public {
  // we check whether there is an article for sale
  require(articleCounter > 0);
  // we check that the article exists
  require(_id > 0 && _id <= articleCounter);
  // we retrieve the article
  Article storage article = articles[_id];
```

```
    // we check that the article has not been sold yet
    require(article.buyer == 0X0);
    // we don't allow the seller to buy his own article
    require(msg.sender != article.seller);
    // we check that the value sent corresponds to the price of the article
    require(msg.value == article.price);
    // keep buyer's information
    article.buyer = msg.sender;
    // the buyer can pay the seller
    article.seller.transfer(msg.value);
    // trigger the event
    LogBuyArticle(_id, article.seller, article.buyer, article.name, article.price);
  }
}
```

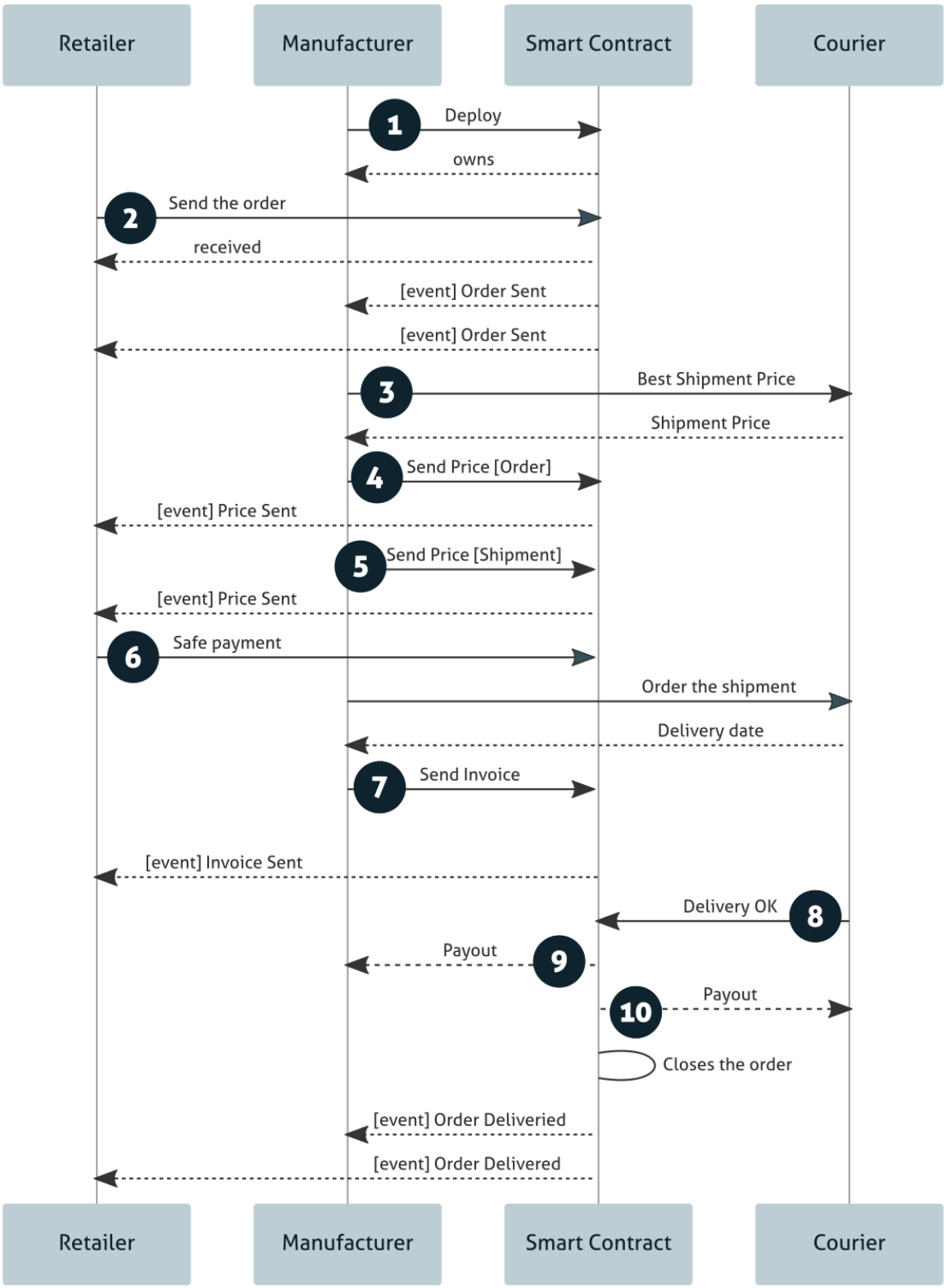

Fig 7: Sequence diagram of Application

To define a sequence of events, external interactions, and payments, I propose a new flow for the case study.

1. The **Manufacturer** deploys the smart contract exclusively for the **Retailer**'s account.
2. The **Retailer** orders *ProductX* with quantity equal to *N* at **Manufacturer**'s smart contract. Through an event, so-called order send, the manufacturers could receive the order data and process it.
3. The **Manufacturer** looks for best shipping price on the **Courier** smart contract.
4. The **Manufacturer** sends the order price and the Retailer receives this through the event called price sent.
5. The **Manufacturer** sends the shipment price and the **Retailer** receives this through the event called price sent.
6. The **Retailer** performs the safe payment of the grand total: order price + shipment price. These coins go to the smart contract account and waits there until the delivery.
7. The **Manufacturer** sends the invoice with a delivery date and some other data. The Retailer receives the invoice data through the event called invoice sent.
8. The **Courier**, after delivery the order to the **Retailer**, marks the order as delivered on the **Smart Contract**. The courier could be a robot, a drone. Think with me! Today we have many possibilities.
9. The **Smart Contract** pays out the **Manufacturer** for the order.
10. The **Smart Contract** pays out the **Courier** for the shipment.

4. Proposed System Analysis and Design

4.1. Introduction

The system makes use of Ethereum protocol based Blockchain. It provides distributed ledger to create legal smart contract. This contract could be used as a legal proof for Retail transactions. The client web application will be used by users to interact with Blockchain. Multiple distributed computing nodes will convert the instated contract into a smart contract which will be encoded and hashed. It will be stored electronically in block which includes

other similar transactions. This block will be validated by other by using algorithm and will be added on Blockchain. This private Blockchain is deployed on peer to peer network using GO Ethereum software.

4.2. Requirement Analysis

4.2.1. Functional Requirements

4.2.1.1. Product Perspective

Minimal transaction costs. It enables the true implementation of continuous deployment in pay-as-you-go mode. The model of big-bulk software licenses or even recurring license fees could be disrupted by micro-transactions for even the smallest deliveries. Very little waste, truly paying for what you use.

Server capable to process the Blockchain transactions and mine blocks.

4.2.1.2. Product features

Minimal agency and contracting costs. Tiny transaction costs minimize also any cost related to contracting either internally or externally. Multi-facet, multi-dimensional and multi-vendor deals become much easier. This of course boosts the decentralization and DAO arguments. Companies can really focus on contracting quality, cost remaining important but weighing less (vs compromising on quality).

Near-instant value transfer. Blockchain facilitates micro-transacting also those occurring in real time. It also expands potential target markets enormously for businesses including almost anyone on earth who is having a mobile phone or has CPU cores.

The product consists of distributed ledger using peer to peer algorithm based on consensus algorithm to create smart contracts and verify validity. It provides

easy accessibility using web based client and simple procedure to sell and buy any product.

4.2.1.3. User characteristics

The user should be aware of the details required to buy and sell a product. The user will be interested in transparent and trustworthy contract which should provide durability and availability. The transactions should be transparent and free from any third party additional charges or fraud. These user concerns are resolved by Blockchain.

4.2.1.4. Assumption & Dependencies

The access to Internet is required. The permission to run peer to peer client for communicating with other clients is necessary and should be allowed by network provider. The smart contract should be able to process the logic for Retail (i.e Buy and Sell of products properly).

4.2.1.5. Domain Requirements

The Retail application should be able to accommodate all types of Real Market Retail transactions and Retail contracts.

4.2.1.6. User Requirements

The application should be able to generate smart contracts for buying and selling of a product and should provide a receipt.

4.2.2. Non-Functional Requirements

4.2.2.1. Product Requirements

4.2.2.1.1. Efficiency (in terms of Time and Space)

Supply Chain: Shipment tracking plays an important role in supply chain. Blockchain can be used to store data about the shipment at every stage of tracking including location, date and time, shipment handling person details, temperature, condition of the package/product, etc. This will help one check in real-time if the shipment has been handled properly and it has arrived on time at any given location. It will also assist the retailers in finding the lost or damaged products in the shipments. During the product recall, an accurate record of supply chain will allow the retailers to identify the source of the issue, the products that are affected, that contain the problems, etc. In addition, Blockchain-based exchanges will allow the retailers to buy or sell from each other as well as distributors through the Blockchain-shared ledger.

4.2.2.1.2. Reliability

Reliability should be high as contracts should be available all time. Usage of Peer to peer distributed ledger guarantees that contract will be durable and available all time.

4.2.2.1.3. Portability

As the web client could accessed through browser, it can be accessed using any Operating system and will be portable across any operating system.

4.2.2.1.4. Usability

The client should be usable and user interface should be user friendly. The non-technical people should be able to create smart contracts for Retail transaction easily.

4.2.2.2. Organizational Requirements

4.2.2.2.1. Implementation Requirements

Network of computers (nodes) are required for computation, competence for validating the transaction and for functioning of proof of work.

The client should have equipment with web browser to access web client.

The Blockchain should be hosted on server with high computation and processing capability.

4.2.2.2.2. Engineering Standard Requirements

Good knowledge of LINUX, API interaction, Blockchain and Data Structure is required. The network should satisfy the peer to peer protocol. The encryption algorithm used should secure the channel cryptographically using algorithm based on public key encryption. Usage of SSL TLS protocol will be preferred.

4.2.2.3. Operational Requirements:

- Economic – Smart contract generation will reduce manual labor to create legal slips will save money and reduce paper wastage. Easier retail process without third party involvement will make products cheaper. Saving contracts automatically on multiple location using block chain would save legal document maintenance cost along with availability and durability.
- Environmental – Paper usage required for creating legal contract will be reduced as contract will be stored in electronic format by usage of few servers.

- Social – The usage of Blockchain increases transparency of retail purchase will increase trust in legal system.

- Political – The usage of fake product delivery and fraud will be reduced by usage of Blockchain.

- Ethical – As contracts are not revertible and can't be deleted or modified, fraud transactions will not be possible and trust in system will increase.

- Health and Safety – Saving of transaction on multiple location will introduce availability and as they can't be modified, trust in system will increase.

- Sustainability – Multiple computing nodes storing ledger will guarantee the availability and durability for legal contract.

- Legality – As the contracts are verified, not revertible and can't be deleted or modified, fraud transactions will be impossible and will reduce the spending on legal matters.

- Inspection ability: Every smart contract is stored in Blockchain as distributed ledger. This can be accessed by anyone who can connect to peer to peer Blockchain network and can prove legality of contract without any significant effort

4.2.3. System Requirements

4.2.3.1. H/W Requirements

- Server – recommended Intel i5 6500 to deploy Blockchain running and windows operating system for deploying Blockchain and serving client app
- RAM - Minimum 4gb RAM requires
- Computer Nodes for Mining of transaction

4.2.3.2. Software Requirements

- Go Ethereum (GETH) – to deploy Blockchain on server
- Solc – to compile smart contract created using solidity language
- Operating system: Mac OS X, Windows, Linux
- Nodejs, Homebrew, Truffle, MetaMask, Ganache
- Ethereum Api, Puppeth
- Text Editor: Atom (recommended)
- PHP server – to server the client and to create GUI application for easy transactions

5. Results and Discussion (As Per IEEE Standard)

5.1. Sample Test Cases (Use standard template for test cases refer Annexure - I)

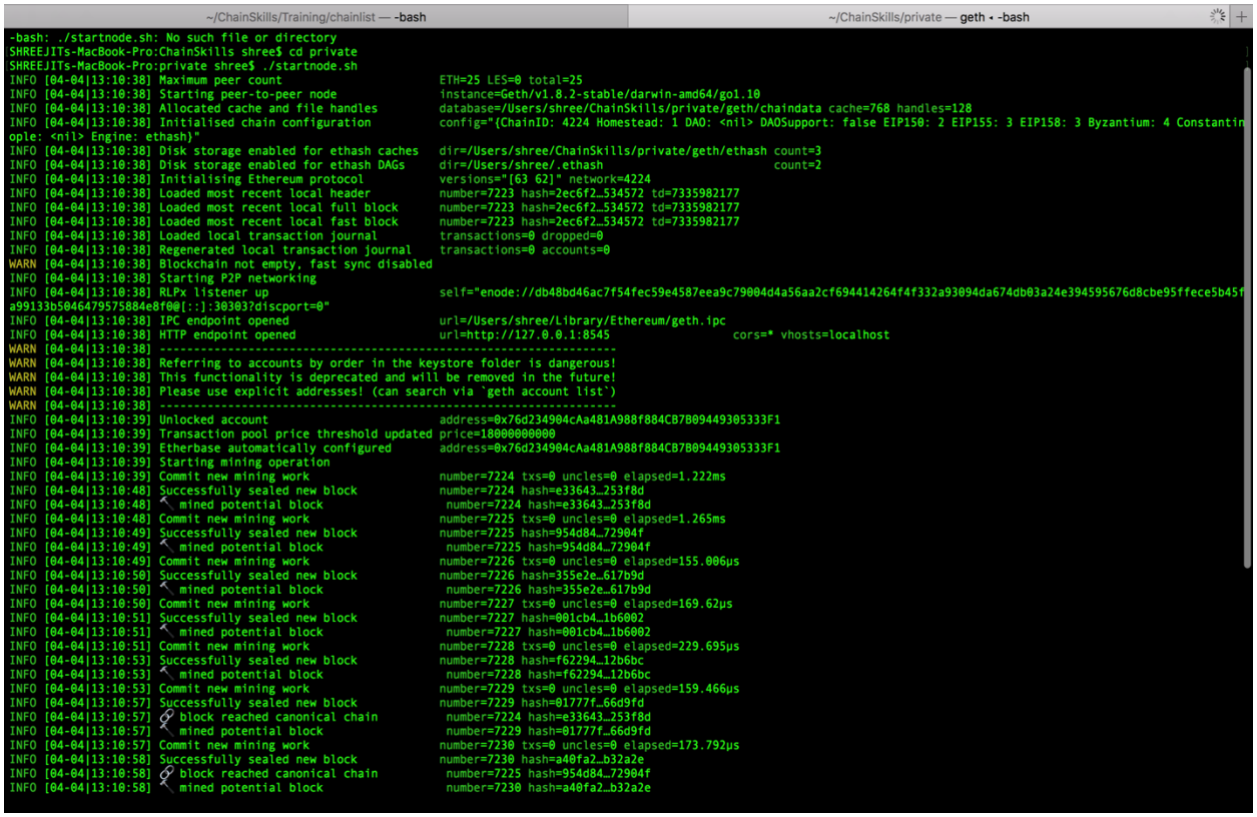

Fig 8: Terminal Screenshot while deploying the Private Node

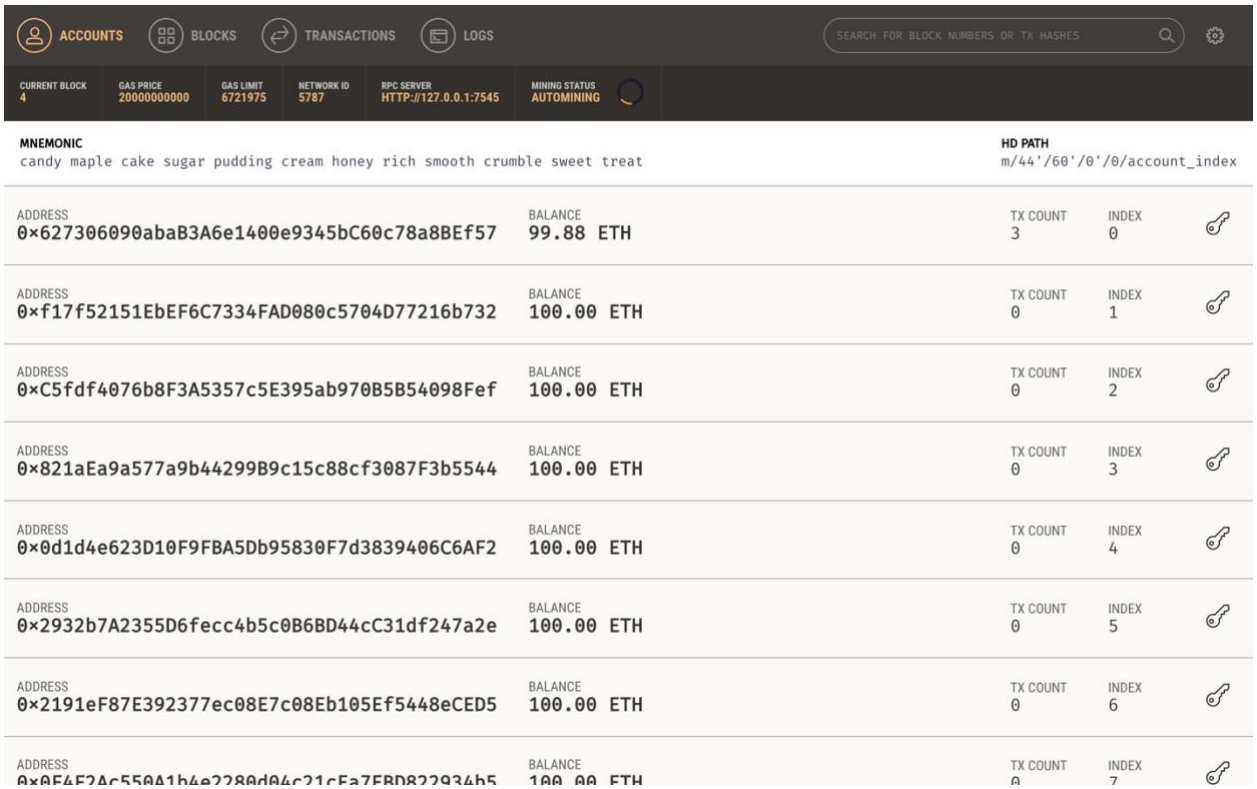

Fig 9: Ganache Screenshot for Accounts Created with their States

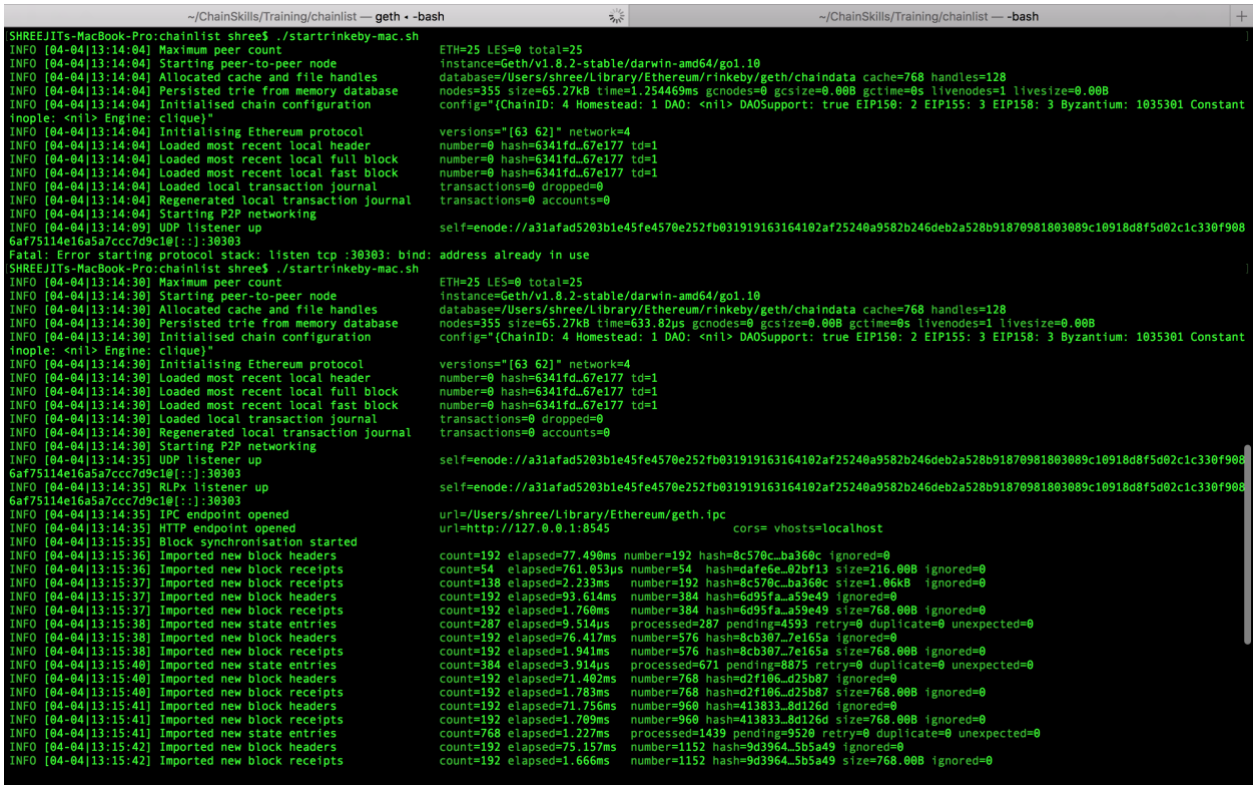

Fig 10: Terminal Screenshot while deploying the Rinkeby Node

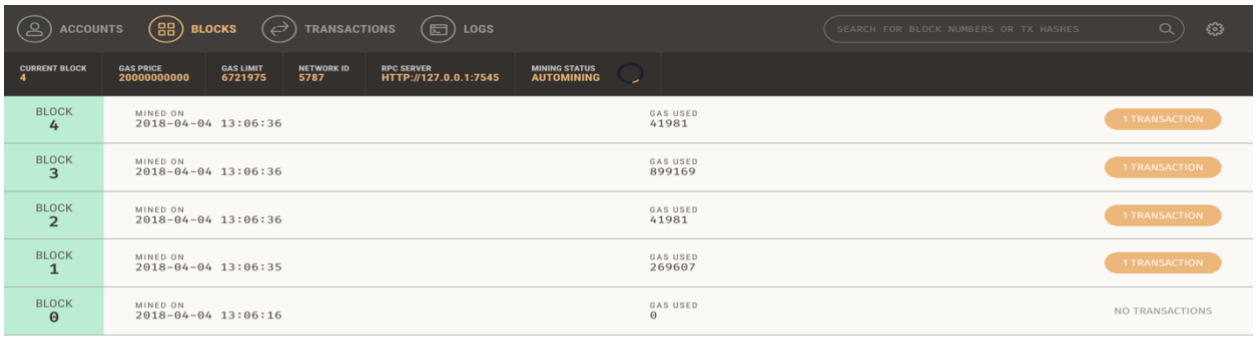

Fig 11: Ganache Screenshot for Block created for Transactions

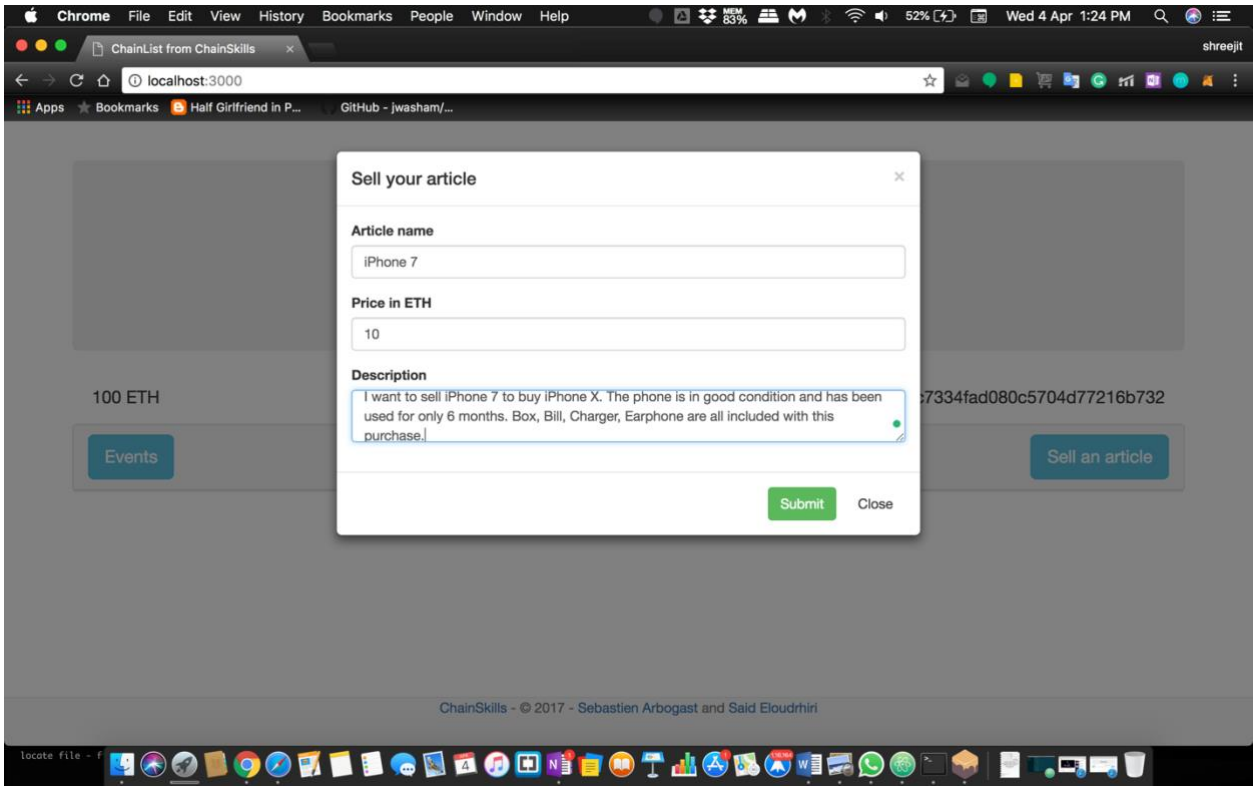

Fig 12: Website Buy and Sell Web front.

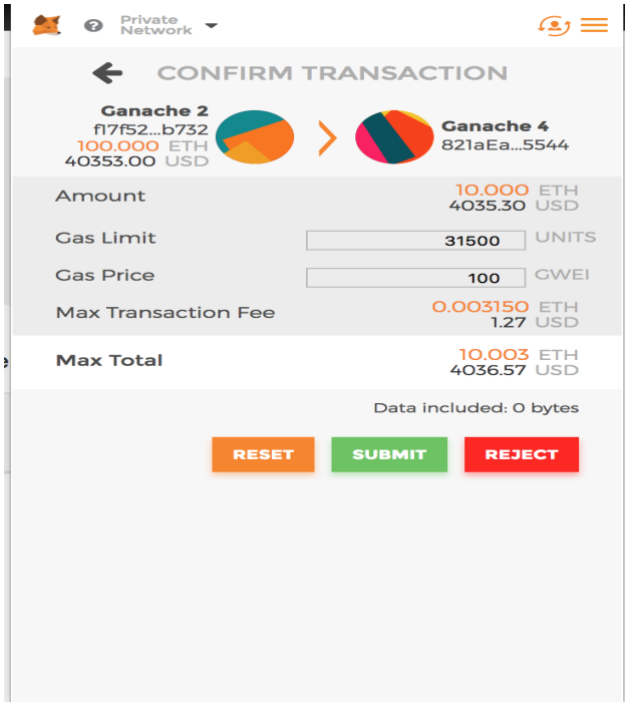

Fig 13: MetaMask Transaction Confirmation Web front.

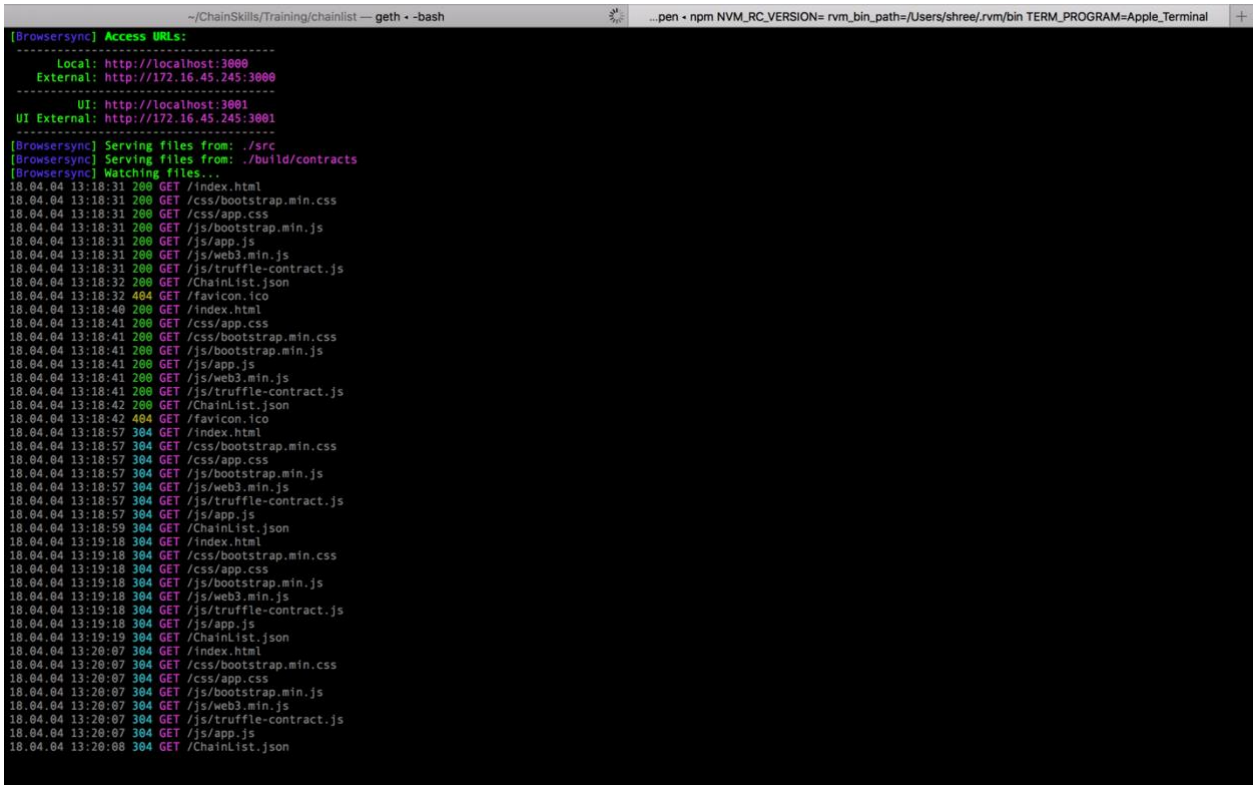

Fig 14: Terminal Screenshot while Transaction blocks are Mined.

5.2. Summary of the Result

CHALLENGES: Blockchain technology is still emerging and is in building era of the proof of concept stage of development and not many Blockchain based systems got deployed at industrial scale, so there are threats with Blockchain and it may still not be fully develop for next few years till it becomes mainstream more. This technology needs to be carefully verified and analyzed before being adopted and its adoption should not be rushed. A failure in implementation may lead to major consequences, and even systemic risks. Being a shared ledger systems, Blockchain is supposed to host sensitive data as well. Hence, it must ensure that its cryptography and cyber-protections are robust and in line with the industry best practices. Data protection and segregation should be taken care of for cloud based retail solutions as well.

The usage of block chain technology for generating smart contract makes process of retail simpler and easy to use. As it uses peer to peer technology and is decentralized, there are very less chance of losing retail information. A person can buy or sell product by creating a contract as a proof of purchase without doing any paperwork. This will also increase transparency of buying and selling of products and provide quicker and easier way to generate proof for purchase without any involvement of third party. Usage of details like Aadhar card will make this process free from hassle.

6. Conclusion, Limitations and Scope for future Work

The decentralized model of Retail market will help to reduce wastage of resource. It helps to reduce paperwork and brings lot of automation with transparency, supply chain collaboration, and power to all. The system is functional only over Internet. If internet is not present, the system becomes inaccessible. If usage of details like Adhaar card is implemented for user identification, it will make the renting any real estate free from hassle.

7. References

Weblinks:

1. https://github.com/ethereum/wiki/wiki/White-Paper
2. https://www.cognizant.com/whitepapers/retail-opening-the-doors-to-blockchain-codex2879.pdf
3. https://www.cognizant.com/whitepapers/how-blockchain-can-help-retailers-fight-fraud-boost-margins-and-build-brands-codex2361.pdf
4. https://www.aciworldwide.com/insights/expert-view/2017/march/blockchain-for-retailers-producing-real-business-benefits
5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf
6. http://www.ethdocs.org/en/latest/
7. https://solidity.readthedocs.io/en/develop/
8. https://www.Blockchain.com
9. https://github.com/web3j/web3j
10. https://github.com/ethereum/solidity
11. https://solidity.readthedocs.io/en/v0.4.21/
12. https://github.com/trufflesuite/truffle
13. http://truffleframework.com/docs/advanced/truffle-with-metamask
14. https://dzone.com/articles/building-a-smart-contract-to-sell-goods

Journals:

1. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org
2. Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
3. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using Blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.
4. Blockchain and its Scope in Retail by Arijit Chakrabarti and Ashesh Kumar Chaudhuri.
5. Blockchain-based Smart Contracts: A Systematic Mapping Study by Maher Alharby, Aad van Moorsel
6. Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016, February). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In International Conference on Financial Cryptography and Data Security (pp. 79-94). Springer, Berlin, Heidelberg.
7. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper.
8. Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using Blockchain platform. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 464-467). IEEE.