Transforming Transactional Marketing of Retailers

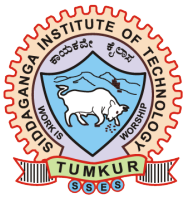
A project report submitted to
Visvesvaraya Technological University. Belgaum, Karnataka
in the partial fulfillment of the requirements for the award of degree of

Bachelor of Engineering
in
Computer Science and Engineering

by

Akashnidhi B Prasad	**1SI15CS007**
Arup Das	**1SI15CS015**
Ashmani Kumar	**1SI15CS017**
Harsh Raj	**1SI15CS042**

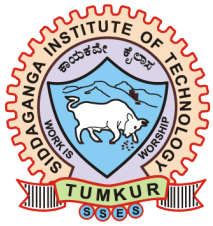
under the guidance of
Mr. A H Shanthakumara
Assistant Professor



Department of Computer Science and Engineering
Siddaganga Institute of Technology, Tumakuru

May, 2019

Department of Computer Science and Engineering
Siddaganga Institute of Technology
Tumakuru - 572103



CERTIFICATE

Certified that the Project Report entitled **"Transforming Transactional Marketing of Retailers"** is a bonafide work carried out by **Akashnidhi B Prasad (1SI15CS007), Arup Das(1SI15CS015), Ashmani Kumar(1SI15CS017) and Harsh Raj(1SI15CS042)** in the partial fulfillment of the requirement for the award of the degree of Bachelor of Engineering in Computer Science and Engineering , Visvesvaraya Technological University, Belagavi during the year 2018-19. It is certified that all corrections/suggestions indicated for the internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering Degree.

.....
Guide and Group Convener
Mr. A H Shanthakumara
Asst. Professor
Dept of CSE, SIT

.....
Dr. R. Sumathi
Professor and Head
Dept of CSE, SIT

.....
Dr. Shivananda K P
Principal
SIT, Tumakuru

Name of the Examiners Signature with Date

1. Prof.
2. Prof.

Department of Computer Science and Engineering
Siddaganga Institute of Technology
Tumakuru - 572103

DECLARATION

I hereby declare that the entire work embodied in this dissertation has been carried out by me at **Siddaganga Institute of Technology** under the supervision of **Prof. A H Shanthakumara**. This dissertation has not been submitted in part or full for the award of any diploma or degree of this or any other University.

Akashnidhi B Prasad (1SI15CS007)
Arup Das(1SI15CS015)
Ashmani Kumar (1SI15CS017)
Harsh Raj(1SI15CS042)
Department of Computer Science and Engineering
Siddaganga Institute of Technology
Tumakuru - 572103

Acknowledgements

We consider this as a privilege to express a few words of gratitude to all those who guided us for the successful completion of our project work.
With reverential pranams, we express our sincere gratitude and salutations to his holiness **Dr. Sree Sree Sivakumara Swamigalu of Sree Siddaganga mutt** for his unlimited blessing.
We express our deep se nse of gratitude, indebtedness and sincere salutations to His Holiness **Sree Sree Siddalinga Swamiji, President, Sree Siddaganga Education Society,** for being a constant source of inspiration in the course of study. We deem it as a privilege to thank **Dr. M N Channabasappa, Director, SIT, Tumakuru** for fostering an excellent academic environment in this institution, which made this endeavor fruitful. We express our gratitude and will remain indebted to **Dr. K P Shivananda, our beloved Principal, SIT, Tumakuru,** for fostering an excellent academic environment in this institution and also providing excellent lab facilities, which made our endeavor possible.We are grateful to **Dr. Shivakumariah, C.E.O, Siddaganga Institute of Technology, Tumakuru** for his kind cooperation and encouragement.
We would like to express our sincere gratitude **Dr. R Sumathi, Professor and Head, Department of CSE, SIT, Tumakuru** for her encouragement and valuable suggestion.
It is a genuine pleasure to express our deep sense of thanks and gratitude to our convener and guide **Mr. A H Shanthakumara, Assistant Professor, Department of CSE, SIT, Tumakuru** as his dedication and mentorship is the key to the successful completion of the project.
Finally we would like to express thanks to our parents ,friends and all those who have directly or indirectly help us in the successful completion of our project.

Abstract

The business sector is an ever-growing sector with the need to satisfy the customer demands alongside making considerable profits for the growth of the industry and self interest. With all the new and upcoming technologies, it was only natural for the commercial businesses like retailers of supermarkets to incorporate emerging technologies like targeted marketing, diversity marketing, transactional marketing and various other strategies to generate more business profit. In the transactional marketing approach the owners of supermarket entice their customers with attractive offers and schemes for growth in their sales. One of the ways was the introduction of shopping coupons by the retail outlets in which the customers were provided with some loyalty points by the retailer on shopping above certain specified amount. These loyalty points could be redeemed by the customer as per the schemes put forward by the retailer.

The development of distributed ledger technology that is, blockchain has led to the emergence of essential applications to payment, clearing, and settlement in the wholesale markets. The responsibility of financial establishments as mediators in trading, clearing and settlements for their customers can be minimised to zero using the blockchain technology potentially decreasing waiting time of huge transactions from days to minutes. The ease of the process of transferring digital currency like Bitcoin and transparency in record maintenance is facilitated by means of peer to peer network, cryptography and distributed data storage.The customers today spend several minutes in the cash counter lines to buy the items that they desire to purchase. It is quite evident that by using technology this time consuming shopping experience can be liberalised to make the shopping experience of the customers more convenient.

One thing common in the way the supermarkets conduct business today is that they offer discounts and issue coupons to customers who shop above a specified amount. This kind of marketing strategy called transactional marketing is effectively applied in supermarkets like more megastores, Big Bazaar, Central, Croma, D-Mart, Hypercity, Reliance Fresh and Westside. But these supermarket retailers maintain a local database at every store which doesnot provide the customer the flexibility to avail the discounts granted to them in other outlets of the supermarket. Moreover the discount schemes in various branches of the supermarket may be different and hence due to lack of awareness of the customer about the several schemes the customer and the business may lose out on their win-win situation. All this is attributed to the absence of a central transparent server connecting all the outlets of the supermarket.Moreover, several customers today have a common complaint on the time spent in the checkout line for purchasing the items from the store that they desire to buy. Our objective is to build a pay as you choose the item.

Our proposed system offers a reward based system using blockchain technology to maintain a blockchain of customers pertaining to an offer proposed by the retailer, common to all the outlets of the retailer and issuance of Value-coins (the cryptocurrency of the reward based system) to the customers on the purchase of every stipulated amount.Our project also aims at simplifying the customer experience when it comes to shopping. The customers today have to stand for several minutes in the cash counter to pay their bills. Such a situation can be avoided by enabling the customer to pay soon after they have finished adding items to their cart. This can be done by enabling the customer to scan the barcodes of the product using their phones and finally pay the total amount.

Our main idea is to make a blockchain of customers for a supermarket which is shared amongst its various outlets along with the accumulation of credits. Our proposed system includes the customer credits provided by the retailer upon shopping above a specified amount, to be accumulated in the customers block. Collectively, such blocks form a blockchain of the customer accounts altogether for the company, which is shared amongst

the network of the company's outlet present in various cities to maintain a proper distributed ledger. The system will allow us to:

1. Make credits called Value-coins with a fixed limit. This limit of how many Value-coins are to be generated in total is decided by the retailer based on the profit margin.
2. Create an autonomous private Blockchain with rules on how many Value-coins will be issued to the customer on spending how much money.
3. Transactions are validated and details of transactions are added to the customer block.
4. In case, the number of Value-coins issued to the customers reaches the limit, it indicates the end of the specific offer scheme.

With the use of blockchain technology the customer would be liberalised from physically possessing discount coupons at the time of redemption, be fully aware of the existing discount schemes and their redemption validity. Thus the use of Blockchain system in supermarkets would ensure a safe, secure and a transparent means for transaction record maintenance and granting of credits to the customer based on the various shopping schemes proposed by the retailer. Moreover, since the concept of blockchain would be used the supermarket retailer would be freed from the cost of maintaining a central server as each time a new transaction occurs the currently active customers could mine them and verify the validity of the transaction.As the idea is to ease the customer experience our aim is also to save the customer's precious time by helping the customer from not standing in long queues of the checkout line. To do this the customer simply needs to scan the barcode printed in the products that he/she desires to buy using their phone, pay for it through their phone and walk out of the store soon after their payment is done.

Contents

Acknowledgements **iii**

Abstract **iv**

List of Figures **xi**

List of Tables **xiii**

1 Introduction **1**
1.1 Background Study 2
1.2 Related Works 2
1.3 Project Problem Statement and Objectives 8
1.4 Organization of the Report 9

2 High-level Design **11**
2.1 Software development methodology 11
2.2 Architecture 14
2.2.1 Architecture Pattern 14
2.2.2 Blockchain Technology Architecture 16
2.2.3 Blockchain Internal Configuration 17
2.2.4 Application Layer Design: User Interface 18
2.3 Incremental Model 20
2.4 Agility and Scrum 21
2.4.1 Why Agility? 21
2.4.2 Agility and the cost of change 22
2.5 Scrum 24
2.6 Functional Requirements 25

2.6.1 Registration of the user in the app . . . 25
2.6.2 Adding product to the cart . . . 26
2.6.3 Adding value coin to the wallet . . . 26
2.6.4 Making payment for the product in the cart . . . 26
2.6.5 Checking Balance of User Wallet . . . 27
2.6.6 Display their Previous Transection . . . 27
2.6.7 Change their credentials . . . 27
2.6.8 Adding Product to the Shop . . . 27
2.6.9 Generation of Barcode for product . . . 27
2.7 Non-Functional requirements . . . 28
2.7.0.1 Accessiblity . . . 28
2.7.0.2 Configuration Management . . . 28
2.7.0.3 Privacy . . . 28
2.7.0.4 Usability . . . 28
2.7.0.5 Availability . . . 29
2.7.0.6 Scalability . . . 29
2.7.0.7 Modifiability . . . 29
2.7.1 Reliability . . . 29

3 Detailed Design 30
3.1 Interface design . . . 31
3.1.1 Login Page Interface Design . . . 32
3.2 Data Structures and Algorithms . . . 32
3.2.1 Block Creation . . . 32
3.2.2 Construction of E-Wallet . . . 33
3.2.3 Block Creation . . . 34
3.2.4 UTXO . . . 35
3.2.5 ECDSA Algorithm . . . 36
3.2.6 SHA-256 . . . 39
3.2.7 Attribute Based Encryption . . . 40
3.2.8 Consensus Mechanism . . . 44
3.3 UML diagrams with discussions . . . 48
3.3.1 Data Flow Diagrams (DFDs) . . . 48
3.3.2 Use Case Diagrams . . . 50

3.3.3 Sequence Diagram 53

4 Implementation **55**

4.1 Tools and Technalogy 55
4.1.1 JSP(Java Server Pages) 55
4.1.2 SQL 55
4.1.3 Database 56
4.1.3.1 MySql 56
4.1.3.2 JDBC 56
4.1.4 IDE 56
4.1.4.1 NetBeans 56
4.2 Experemantal Setup 56
4.3 Coding Standerd Followed 57
4.4 Functional Implementation 58
4.4.1 Register/Signup 58
4.4.2 Scan Product Barcode 59
4.4.3 Checkout/Payment 59
4.4.4 View sell history 59
4.4.5 Release Token 59
4.4.6 Checking validity of token 59

5 Testing **60**

5.1 Test workflow 60
5.1.1 Unit Testing 60
5.1.2 Integration Testing 61
5.1.3 Validation Testing 62
5.1.4 Regression Testing 62
5.1.5 Sanity Testing 64
5.2 Test case details 64
5.2.1 Test case id: Creation of Genesis Block 64
5.2.2 Test case id: Making a transaction 65
5.2.3 Test case id: Creating a barcode 65
5.2.4 Test case id: Reading values from barcode 65
5.2.5 Test case id: Adding coins into the wallet 66

6 Conclusions and Future Scope **67**

Bibliography **69**

List of Figures

2.1 Software Development Life Cycle 12
2.2 Layered Pattern Architecture 14
2.3 Blockchain Technology Architecture 16
2.4 System Architecture 18
2.5 Incremental model for project 20
2.6 Agility and the cost of change 23
2.7 Scrum design of project 24

3.1 User Interface for both Web and Mobile. 32
3.2 Illustration of UTXO transactions 36
3.3 SHA-256 41
3.4 Message trades of Aura and Clique PoA for each progression. In this model, there are 4 experts with id 0,1,2,3. The pioneer of the progression is specialist 0. 46
3.5 Selection of participants enabled to suggest blocks in Clique. 47
3.6 A fork happening in Clique. 47
3.7 Level 0 DFD. 48
3.8 Level 1 DFD. 49
3.9 Level 2 DFD. 50
3.10 Overall Use Case Diagram. 51
3.11 Overall Sequence Diagram. 53

5.1 Unit Testing 61
5.2 Integration Testing 61
5.3 Validation Testing 62
5.4 Regression Testing 63

5.5 Regression Testing 63

List of Tables

3.1 Comparison of various Consensus Algorithms 45

Chapter 1

Introduction

The business area is a regularly developing division with the need to fulfill the client requests nearby making impressive benefits for the development of the business and personal responsibility. With all the new and upcoming innovations, it was normal for the business organizations like retailers of grocery stores to fuse developing advances like focused on promoting, decent variety showcasing, value-based advertising and different procedures to create more business benefit. In the value-based showcasing approach, the proprietors of store allure their clients with appealing offers and plans for development in their deals. One of the ways was the presentation of shopping coupons by the retail outlets in which the clients were furnished with some dependability focuses by the retailer on shopping over a specific determined sum. These devotion focuses could be recovered by the client according to the plans set forward by the retailer. With the rise of innovation each speculator today is enthused about diminishing the work cost and increment their net revenues. Lessening the expense on work will empower the representatives to get higher additions from their organizations and grow their market. The present retailer outlets include a ton of easygoing workers. Infact in excess of nine lakh American representatives are viewed as easygoing workers in such outlets. With the utilization of innovation on the off chance that one could truly computerize the whole procedure of purchasing merchandise from such outlets then the future retailers would appreciate benefits more than what the outlet business is putting forth the retailers today.

1.1 Background Study

One thing basic in the manner in which the stores direct business today is that they offer limits and issue coupons to clients who shop over a predetermined sum. This sort of promoting methodology called value-based marketing is successfully connected in markets like more megastores, Big Bazaar, Central, Croma, D-Mart, Hypercity, Reliance Fresh and Westside. Be that as it may, these market retailers keep up a nearby database at each store which doesn't give the client the adaptability to profit the limits conceded to them in different outlets of the general store. In addition the markdown plots in different parts of the general store might be extraordinary and henceforth because of absence of attention to the client about the few plans the client and the business may miss out on their winâĂŞ win circumstance. This is credited to the nonattendance of a focal straightforward server interfacing every one of the outlets of the general store.

Also, a few clients today have a typical grumbling on the time spent in the check-out line for acquiring the things from the store that they want to purchase.

1.2 Related Works

Title of the Work: To Blockchain or Not to Blockchain; That Is the Question
Authors: Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Victor Santamaria
Publication Details:IEEE Computer Society On March/April 2018
Description:This paper answers one of the most basic question:"What is blockchain?" BlockChain is a public ledger having record of all transactions and distributed among network participants where every transactions before being added to the ledger is being verified by the other participants according to the majority consensus mechanism. This records cannot be changed or edited once added to the ledger. Advantages of using blockchain include following features: Data Security: Since data is shared among all the participants of the network, if in any unfortunate case data is lost, it can be recovered using other participant's data. Transparency: Everyone has the access to all the history transactions. Decentralization: There is no place for the central authority to control the network. Disadvantages of using blockchain include High

power computation. Mining require expensive hardware. Only one miner wins others resources are wasted. Data replication requires space. Local copies of all transaction are stored on each network node. Adding new information are very slow. Transparency may affect the privacy of the user. One should use blockchain when there is a requirement for (i) Shared database. (ii) Many writer nodes. (iii) To see the connection between the transactions. This paper helped us to get confidence about using the blockchain for our idea. This paper told us about the features about the blockchain such security, decentralisation, etc. [1]

Title of the Work:A Blockchain-Based Access Control System for Cloud Storage

Authors:Ilya Sukhodolskiy, Sergey Zapechnikov

Publication Details:IEEE Computer Society On 2018 Issue No. : 978-1-5386-4340-2/18

Description:Since the number of users of cloud-based services have used, problems regarding the security and copyright aspects has increased. Most effective way to secure is to encrypt the data before uploading those, which is recommended by the Cloud Security Alliance. There are certain difficulties in imposing the encryption and accessing the data to use them. Some of the tools to encrypt files before sending them to the cloud is BoxCrypt, CryptDB, ARX. To ensure the data integrity and non-repudiation on the distributed cloud system is BigChainDB. One way is to introduce the decentralized scheme to control the access to encrypted data. Mate Horvath proposed in a multi-authority CP-ABE scheme for effective revocation of user's attributes based on their identities. Most of the functions are performed on the client side because exchanging of the data are mostly private. Remaining functions are performed using the smart contracts in the Ethereum Virtual Machine. Benefits of using the access control system is that it provides the ability to change the accessing policy for the encrypted data without duplicating it; integrity of information about the transactions which includes the granting and changing the access and many more. The entire concept discussed in this paragraph can be vividly studied in paper. This project helped us to reach the conclusion about the storing the data of the blockchain in cloud.[2]

Title of the Work:(Block) Chain Reaction

Authors:Leslie Mertz

Publication Details:IEEE Pulse Issue No. 2154-2287, 15 May 2018

Description:Use of blockchain in the field of healthcare to maintain a health ledger, which have all the data of the patients from physician to get the patient's pertinent medical information, which can be used in future. But challenge here is to get all the data from all physician because a person may consult to many doctors from different for different problems. Blockchain can be useful in the other aspects of healthcare such as insurance claims and other administrative problems of estimating health related population data. Any data once added to blockchaincannot be changed or deleted, property of blockchain, ensure that the data are correct and changed. Mari Greenberger, director of informatics in HIMSS, North America believes that blockchain have immense potential that can help with critical components. HIMSS has started to work in blockchain to dig out the best features of blockchain that can be proved very useful in the field of healthcare. They stated the problems in using blockchain for healthcare is that hesitation to use new technology , privacy and security concerns. Carter of the blockchain research institute says that "Better outcomes are derived from better data" and right now if we create blockchain to create commons and individual control their data and other healthcare bodies are allowed to access them, it will help them in long run. This provides a detailed study on the above discussed content. This paper gave us the brief idea about the blockchain. It features and use of blockchains and its definition. [3]

Title of the Work:Blockchain and Smart Contract for Digital Certificate

Authors:Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen

Publication Details:IEEE International Conference on Applied System Innovation2018, Issue No. : 978-1-5386-4342-6

Description:As indicated by the Taiwan Ministry of Education insights, numerous understudies travel to different nations for further investigations or change states because of a few reasons or because of some work prerequisites. Because of inaccessibility of any enemy of fashioning techniques, there have numerous cases which have seen produced declarations cases. To counter this issue, blockchain can be utilized to make computerized endorsement. By the property of non-alteration, advanced declaration having hostile to fake and certainty can be made. System of making the computerized declaration is , create the electronic record of a paper authentication going with other related information into the database, in the mean time figure the electronic document for its hash esteem. At long last, store the hash an incentive into

the square in the chain framework. The framework will make a related QR-code and request string code to attach to the paper testament. It will give the interest unit to confirm the validness of the paper authentication through cell phone examining or site request. This data illustratively clarifies this idea. This gave us idea how digital signature and smart contract can be used simultaneously to provide more better security. This idea was used to compare different ideas to secure the data according the complexity and resource available. [4]

Title of the Work:The Use Of Distributed Ledger Technologies in Payment, Clearing and Settlement

Authors:Lael Brainard

Publication Details: Board Of Governors Of The Federal Reserve System at Institute Of International Finance Blockchain Roundtable, Washington D.C. in April 14, 2016

Description:The advancement of circulated record innovation that is, blockchain has prompted the development of basic activities in leeway and business in the discount markets. The obligation of banking foundations being arbiters in making buys and settling client bills can be limited to zero utilizing the blockchain innovation possibly diminishing holding up time of gigantic exchanges from days to minutes. The simplicity of the way toward exchanging computerized cash like Bitcoin and straightforwardness in record upkeep is encouraged by methods for shared system, cryptography and circulated information stockpiling. This paper was gave us the idea about the one of the different transactions methods available using blockchain. This was used to compare with different ways available. [5]

Title of the Work:Introduction to Security and Privacy on the Blockchain

Authors:Harry Halpin and Marta Piekarska

Publication Details:2017 IEEE European Symposium on Security and Privacy Workshops (Euro S and PW)

Description:There are different focal points of applying blockchain to publicize theories. The profitable trade and association of trade nuances between the merchant and the buyer is extremely essential and safe with the blockchain development. At any rate there are issues related to enduring quality and separated utilization of blockchain advancement. Some genuine concerns identifying with blockchain are 51 percent attack, idleness of the framework and framework transmission limit. The

game plans contrasting with such issues have been enough found and enlisted. This paper was helpful and it helped us to reach the conclusion to use blockchain for our domain of marketing and maintaining the transactions. [6]

Title of the Work:A Brief Survey of Cryptocurrency Systems

Authors:Ujan Mukhopadhyay, Anthony Skjellum, Oluwekemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks

Publication Details: IEEE

Description:The blockchain can be utilized to give answers for issues relating to spaces that may appear to be absolutely superfluous. Some these spaces could incorporate administrations in the administration division, organizations, secure verification and approval. Decentralized applications called 'DApps' can keep running on both customer side and on the blockchain. There are different cryptographic forms of money like ethereum, bitcoin, journalcoin, learncoin, healthcoin and a lot more whose unmistakable qualities and strong point is introduced in the paper. This paper work gave us the idea about how to store data in blockchain in encrypted format and to choose from different encrypting methods available. [7]

Title of the Work:Bitcoin mining acceleration and performance quantification

Authors: Electrical and Computer Engineering (CCECE)

Publication Details: 2014 IEEE 27th Canadian Conference on 4-7 May 2014, INSPEC Accession Number: 14599397

Description:Bitcoin mining is genuinely fundamental to improve the security of the exchanges. As the quantity of bitcoin diggers expands the trouble of the math issue to be settled additionally increments. There are different techniques for performing Bitcoin mining. The noteworthy tasks of SHA-256(Secure Hash Algorithm-256) hashing of qualities to change over the information into a sheltered and secure unique mark of that information has been viably explained in the paper. [8]

Title of the Work:Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms

Authors:O'guzhan Ersoy, Zhijie Ren, Zekeriya Erkin and Reginald L. Lagendijk

Publication Details:2018 Crypto Valley Conference on Blockchain Technology

Description:There is an intensive wastage of resources when it comes to the usage of blockchain especially the process involving the mining of the blockchain. Blockchain mining wastes a lot of energy. Mining in blockchain is prone to the very famous 51

percent attack which can easily happen in smaller blockchains. The idea behind the acceptance of a particular blockchain from the different versions of the blockchain is choosing the chain of longest length. This means that for a malicious miner to take advantage of double spending must have a computation power greater than most of the miners in the blockchain so that it can add more blocks than the other true miners and hence get the false blockchain into acceptance by the other miners as soon as length of blockchain created by the miner is greater than the length of the original blockchain. Considering the fact that there are thousands of miners available on the blockchain, a malicious miner would have to spend enormous amounts of money on mining hardware to compete with the rest of the network. Even the strongest computers on earth are not directly competitive with the total computational power on this network. Thus the size of the network plays a key factor in preventing 51 percent attack. Faster throughput and lesser latency are what the blockchain technology demands for its efficient functioning. There are certain challenges regarding the scalability of the blockchain that also needs to be dealt with. This helped us to choose between different types of consensus algorithm and their advantages and disadvantages. [9]

Title of the Work:A Scale-out Blockchain for Value Transfer with Spontaneous Sharding

Authors:Zhijie Ren, Kelong Cong, Taico V. Aerts, Bart. A.P. de Jonge, Alejandro F. Morais and Zekeriya Erkin

Publication Details:978-1-5386-7204-4/18 IEEE

Description:Blockchain additionally experiences numerous telecom of a similar exchange over the system. Every exchange is first checked before including into the block. So before the confirmation each exchange is a piece of the unconfirmed pool of exchanges. So as to keep away from excess in the hinders a convention called first-pioneer then-block accord convention is utilized. This proposition lessens the correspondence cost by practically 97 percent when contrasted with the genuine correspondence norms which are as a result today. This paper only examines the fulfilling or the motivating force systems embraced for exchange expense proliferation which is free of the system topology. The different ideas featured here are I-associated systems, Eclipse and parceling, engendering lemma and the value lemma. This paper

brief us about the way of storing data in blocks and pros and cons. [10]

1.3 Project Problem Statement and Objectives

Our proposed project offers a reward based scheme utilizing blockchain innovation to keep up a blockchain of clients relating to an offer proposed by the retailer, normal to every one of the outlets of the retailer and issuance of Value-coins (the digital currency of the reward based framework) to the clients on the buy of each stipulated sum.
Our undertaking additionally goes for rearranging the client experience with regards to shopping. The clients today need to represent a few minutes in the money counter to pay their bills. Such a circumstance can be kept away from by empowering the client to pay not long after they have completed the process of adding things to their truck. This should be possible by empowering the client to check the scanner tags of the item utilizing their telephones lastly pay the aggregate sum.
Our fundamental thought is to make a blockchain of clients for a supermarket which is shared among its different outlets alongside the amassing of credits. Our proposed framework incorporates the client credits given by the retailer after shopping over a predetermined sum, to be collected in the clients square. All in all, such squares structure a blockchain of the client accounts inside and out for the organization, which is shared among the system of the organization's outlet present in different urban areas to keep up an appropriate circulated record. The system will allow us do the following things:

- Make credits called Value-coins with a fixed point of confinement. This point of confinement of what number of Value-coins are to be produced altogether is chosen by the retailer dependent on the net revenue.
- Exchanges are approved and subtleties of exchanges are added to the client square.

- In case, the number of Value-coins issued to the customers reaches the limit, it indicates the end of the specific offer scheme.
- A client will certainly make a bill just by examining the barcode present on the item and make payment by means of app itself without experiencing the long queue and squandering imperative time.

With the use of blockchain technology the customer would be liberalised from physically possessing discount coupons at the time of redemption, be fully aware of the existing discount schemes and their redemption validity. Thus the use of Blockchain system in supermarkets would ensure a safe, secure and a transparent means for transaction record maintenance and granting of credits to the customer based on the various shopping schemes proposed by the retailer. Moreover, since the concept of blockchain would be used the supermarket retailer would be freed from the cost of maintaining a central server as each time a new transaction occurs the currently active customers could mine them and verify the validity of the transaction.

As the idea is to ease the customer experience our aim is also to save the customer's precious time by helping the customer from not standing in long queues of the checkout line. To do this the customer simply needs to scan the barcode printed in the products that he/she desires to buy using their phone, pay for it through their phone and walk out of the store soon after their payment is done.

1.4 Organization of the Report

Chapter 1, contains the prologue to the undertaking.

Chapter 2, gives us knowledge into the plan utilized in the task. It gives us the procedure utilized for programming improvement, the engineering utilized in the undertaking, it additionally gives data about each capacity utilized in the task.

Chapter 3, Detailed Design, gives us the thought regarding the Interface plan, information structure used to take care of the issue, Use case chart and different

subtleties.

Chapter 4, ie Implementation, gives us the data about the Tools and Technology utilized for the fruitful consummation of the undertaking, coding standard utilized in the task, Implementation work process and non-useful necessities and code reconciliation subtleties.

Chapter 5, ie Testing, gives us the thought regarding the testing plan pursued checking off the task full usefulness.

Chapter 6, ie Conclusion and Future Scope, expresses the accomplishment made by the individuals towards the fruition of the destinations and what might be the future employment of this undertaking.

Chapter 2

High-level Design

This module discusses the software engineering model that this project is developing.oped. First, we have an incremental model that contains briefly current version of Smart Shop has been implemented. then,A description of agility means a regular briefing on project status.The faculty panel and our respected guide. Then for ScrumThat is, regular meetings held by team members.

2.1 Software development methodology

Software development life cycle is the product confguration, make and trial Best notch programming. SDLC means transmitting superior programming that meets or exceeds customer needs, Completion of completion of internal conditions and cost means. SDLC is a technology. Taken for product planning within the product association. It contains the core. Harsh preparations depicting how to create, maintain, replace, and enhance specific methods programming. The following diagram is a graphical illustration of the various stages. The detailed SDLC diagram of this report shows that all steps We worked together to ensure that the proposed tasks were accurate and accurate. Typical The software development life cycle(SDLC) consists of the following steps:

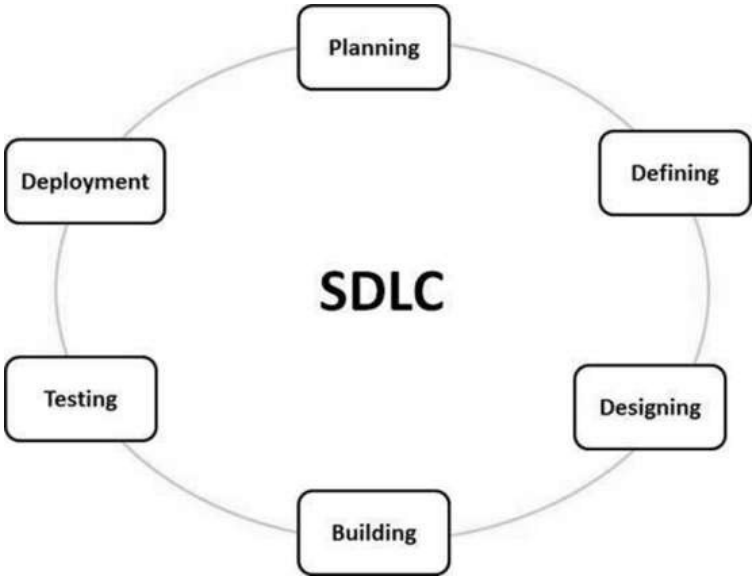


Figure 2.1: Software Development Life Cycle

- **Stage 1: Planning and Requirement Gethering**
  The set of requirements is one of the most important and important steps in SDLC. It is a group of senior executives who have made significant contributions from clients, business offices, advertising, and business space experts. These data are used to design basic working methods, to derive elements, and to think in highly operational, specialized areas. A course of action is created to provide good quality of life necessities and to identify evidence of threats associated with roaming in the main phase. I think the outcome of a particular commodity will be a brief risk, namely describing a specific way of insight that can be taken to properly understand the tasks.

- **Stage 2: Defining Product Requirements**
  Once the basic check is complete, the next step is a clear imaging. Report what you need and have your customer support it. Or market agent. This includes everything you need to do through the Software Requirements Specifications (SRS) report. It was made in the middle of the life cycle of the business.

- **Stage 3: Devloping the End Product Architecture**
  The collation approach clearly describes all units of the plan for near-by-correspondence

and filming the data stream with external units that can not be compromised (expect any). Under a large number of proposed design units, they should be clearly described with less unclear components in DDS.

- **Stage 4: Developing the Product**
  True change begins and ends in this SDLC era. Programming code is generated by DDS in the middle of this step. If an order is executed and processed in a positive way, the main code may become an older problem. Planners should leverage the coding rules represented by documentation and programming tools such as transcoding tools, intermediaries, and debuggers. For example, language programming languages such as C, C ++, Pascal, Java, and PHP are used. Coding. The programming language is chosen in relation to the types of computer software writing that have already been delivered.

- **Stage 5: Testing the Product**
  This step is usually a subset of the broader steps as in the front. In line SDLC models, testing practices in general in each Of the SDLC time period. Nevertheless, the step and this will simply offer the test period. In the represented thing, it takes, to its apex This work must perform a quality measurement described in the SRS.

- **Stage 6: Deployment and Maintenance**
  Once the work has been tried and delivered, it is formally released. At the right market. The process of resending from now on will proceed to the following steps. It is indicated by the business strategy of the partnership. At first, Released in limited areas and attempted in certification business terms (UAT-user verification test). Until then, from the point of view of information, It can be released intact or with intensive changes proposed. Promote parcels. After the item is released in the market, its maintenance is strengthened. The situation is current customer base.

2.2 Architecture

This document provides a high level overview and explains the architecture of the Smart Shop System.

The record characterizes objectives of the design, the utilization cases upheld by the framework, structural styles and parts that have been chosen. The archive gives a justification to the engineering and structure choices produced using the theoretical plan to its usage.

2.2.1 Architecture Pattern

Their are generally three type of architecture pattern supported in the blockchain.

- **Layer pattern:**

  Layer pattern architecture helps to structure applications that can be decided

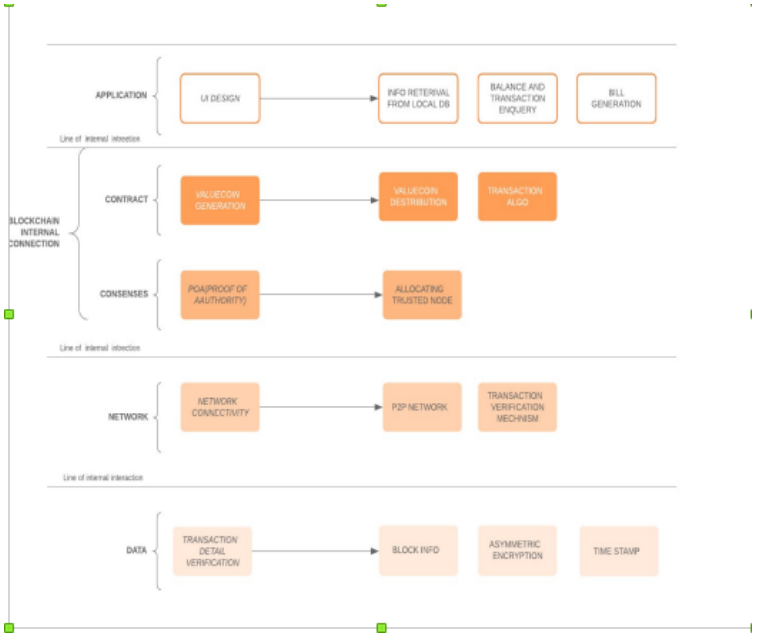


Figure 2.2: Layered Pattern Architecture

into different subtask .The layers can be divided according to the OSI layers, different components (modules), protocols. A large system needs decomposition. Blockchain is a very vast system and its implementation has very different

components which can be divided into different layers, each layers can be represented by a CRC card having class name as the layer name .

- **Pipeline and filter pattern:**
  This architecture provides structure for system that process a stream of data. Each step is encapsulated with a filter component and the best example of this system is a parser. This type of system is used when we want to compute a stream of data for ex lets take the parser of a compiler, the ASCII value is passed bit by bit from a lexical analyzer which converts it to a token stream then in the next step it is passed through the syntax analyzer in which it is filtered and then checked for any syntax error and so on. The filter component is the processing unit of the pipeline. Filters enhance, enhance, or convert the input data. It transforms data by calculating information, adding information to enrich the data, concentrating or extracting information to materialize the data, and delivering the data to other representations. Specific filter implementations can combine any of these three basic principles.

  - The pipeline component pulls output data from the filter
  - The previous pipeline element pushes new input data in the filter
  - filter is the very active member it is responsible for pushing in and pulling out the data from the pipeline.

  The CRC card of this data can be represented using two cards with class filter and pipeline. The data flow diagram(DFD) can be drawn to explain the flow of the process between the pipeline and filter.

- **Blackboard pattern:**
  The blackboard architecture pattern is helpful for problems in which the solution is non deterministic. For e.g. let us consider the speech recognition technique where the speech is converted to text by prediction of the wavelength of the voice. In this architecture is divided into two components blackboard and knowledge source. The speech recognition system contains a variety of knowledge sources that shift the individual hypothesis to a higher level with multiple hypotheses and consecutive time intervals at the same level. For example, a

statement is created by choosing words that span the interval that corresponds to this statement. Other sources of knowledge predict new hypotheses at the same level. For example, the source of knowledge foretells potential words that can be preceded or followed by a particular phrase. We also identify the source of knowledge that validates the expected hypotheses based on the information in the next sub-step. Consistency is calculated between a set of segments that extend in the same time period of the expected word. The control component monitors the changes on the panel and performs a loop that specifies what to do next. Schedule evaluation and activate knowledge sources according to the strategy of applying your knowledge. The basis of this strategy is the data on the blackboard. This technique cannot be used for our implementation of block chain as we need to have a deterministic solution.

2.2.2 Blockchain Technology Architecture

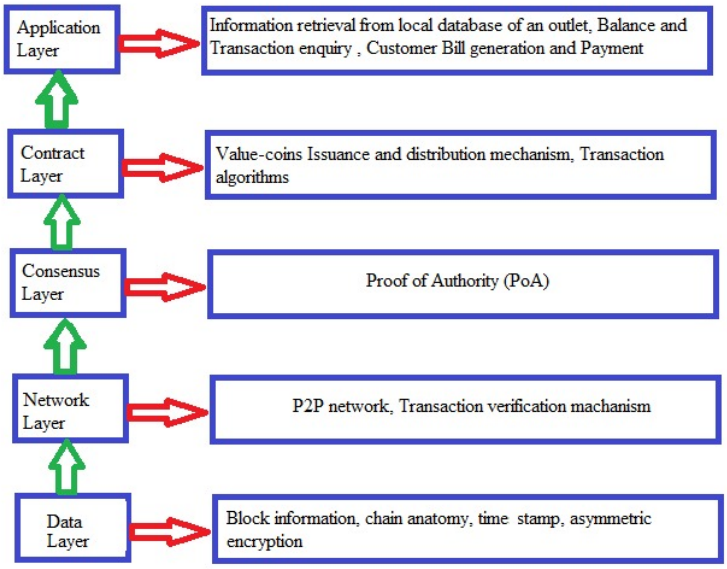


Figure 2.3: Blockchain Technology Architecture

There are five conceptual layers of blockchain: data layer, network layer, consensus layer, contract layer and application layer [2]. The data layer contains the block data, structure of the chain, customer address data, time stamp of block creation and details

of asymmetric encryption. It is because of the data layer that transactions can happen transparently in a non-repudiated and authenticated manner. The networking layer makes sure that each node receives transactions. The consensus layer makes sure that each node agrees on the same transactions to modify their local state. The contract layer is responsible for checking the credit limit of the customer in order to make a successful transaction. It ensures a safe and secure transaction, issuance and distribution of Value-coins by the genesis block. As for the application layer, it processes transactions. Given a transaction and a state, the application will return a new state. Each transaction abides by the norms of the contract layer and modifies the state according to the specific transaction rules.

2.2.3 Blockchain Internal Configuration

blockchain is the transaction database that is shared by all nodes involved in the Bitcoin-based system. The entire copy of the currency block string contains each conversion performed in currency. You can use this information to determine the value per title at any time in history. Each block contains the segmentation of the previous block. This has the effect of creating a series of clusters from the configuration to the current cluster. Because the previous cluster fragmentation is unknown, each block is served after the previous cluster. Each block is not practical for calculation once it is modified once in the chain. This is because you have to update each block afterwards. These properties make block-chained transactions irreversible. As we know that blockchain uses linked list data structure for storing data.Each block in blockchain stores details about the previous block hash function Fig 1 gives the overview of connection between blockchain. In each block we store details about various details about user the details about user is as follows

- **Previous Block Hash:** it stores the previous block hash in blockchain. It is used to make connection between different blocks by using Linked list data structure
- **Nonce:** It is a 32 bit arbitrary random number that is typically used once. It is basically used for calculation of has value of current block.

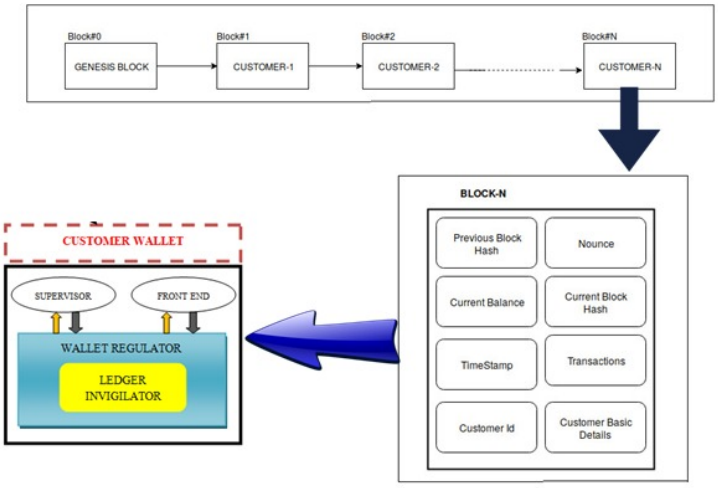


Figure 2.4: System Architecture

- **Current Balance:** It indicates the amount of un-spent Value-coins present in the wallet.
- **Current Block Hash:** It is calculated by hashing the value of nonce, previous block hash, Timestamp value by applying SHA256 algorithm.
- **Time Stamp:** Every block in blockchain contains a Unix time timestamp. In addition to being used as a source of transforms for block hashes, it makes it more difficult for the enemy to manipulate the block chain.
- **Transactions:** Inside each block we store receipt of purchase inside a block in SQL format of fixed length.
- **Customer id:** It is a uniquely identity for each customer in blockchain
- **Customer Contact Details:** We store the basic contact details such as mobile number, name, address etc

2.2.4 Application Layer Design: User Interface

UI of our application will be made for Android using Android Studio. It will first have a login and signup page. New user have to login into our system and provide all the required details during the signing up. All the details asked will be useful

for running our application successfully and reaching the expectation. Once signup procedure is completed, user have to login again into the system via the application using their credentials. Customers can also change their credentials again afterwards according to their wish and comfort.
Our application will be having following options:

- **Make some transactions:** After doing all the shopping they can just pay the amount, displaying below the cart. Payment will be made using the ValueCoins present in the wallet.
- **Check their balance**After making all the payment or before shopping customer can check their balance.
- **See their past transactions:** It will show the list of transaction made. It will contain only up-to certain number or certain time. It will have details of the transaction such as coins spent, products taken, coins rewarded for shopping.
- **Add coins(money) to their wallet:** Since all the payment will be done using our made currency ie ValueCoins. We must add money to our application in the wallet provided. It will convert all the currency into ValueCoins as per the rate decided before.
- **Add and delete something to and from cart respectively:** While in shops/marts customer can add some products into their cart by scanning the QR code on the product and keep it with them. And if they feel that some product are useless to them or not necessary, they can delete the item from their cart just using the remove option available to every item present in the cart and the corresponding item will be removed.
- **Check the list of items in cart:** Customer can at anytime see the number of items available in their cart and can decide whether to shop more or not. And can even mange their checklist and it will also show the total cost of the cart and can decide further.
- **Change their credentials:** If one customer feels like one should change their credentials, they can by just providing certain details which will be available only with the authorized user.

2.3 Incremental Model

What the incremental frame shows is a strategy for programming behavior. The work is made progressively (up to several degrees, executed, and endeavored. More is integrated each time) until the end of the work It joins change and change. The thing is described as follows. It accomplishes the more prominent part of its necessities. This shows the integration. The section of the waterfall appears as a repetitive basis for prototyping. Work Each part is weakened to a unique part that is organized and manufactured. unreservedly (named as a collection). Each part is passed to the client upon completion. This gift lacks the utilization of things and maintains a strategic distance. Long progress time. Continue to remove the key as you do with the important start. Capital receives tolls and guarantees a wide hold period. this is advancement in expansion at the same time is a completely modern system.

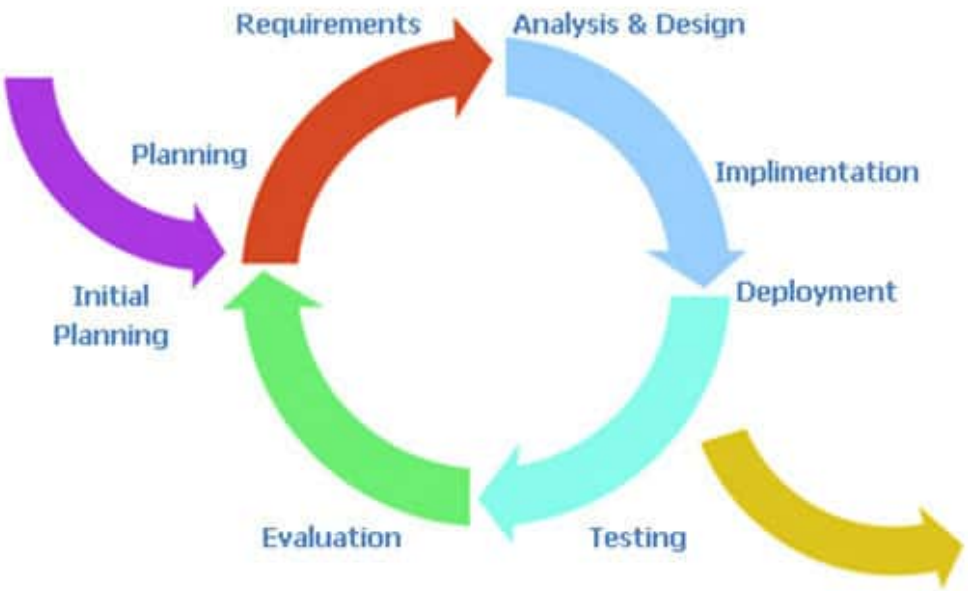


Figure 2.5: Incremental model for project

Properties of Incremental Model:

- System is isolated into various small headway wanders.

- Partial systems are com to convey the final framework.
- First dealt with most essential require necessities.
- The prerequisite of a portion is cemented once the expanded bit is produced.

The reverse slew test should be easy for each cycle. In the middle Testing, the damaged parts of things can be quickly seen in terms of several ways The changes are highlighted internally. Testing is much easier. Explore other strategies for programming motion in that light. The most important part is that less change occurs in the middle of each emphasis. This makes the inside of each part more focused and seriously tested. Common point. It looks like the customer has responded to the highlights and outlines what they used. Required changes. Essential movements are fast and cost-effective in the incremental model.

2.4 Agility and Scrum

Agile is a time-driven, iterative approach to delivering software that gradually builds software from the beginning of the project, instead of delivering everything at once.

2.4.1 Why Agility?

The current technology age is faster than ever, and global software companies are forced to work in a rapidly changing and changing environment. Because these businesses operate in a constantly changing environment, it is impossible to capture a complete and thorough set of software requirements. Without these requirements, all existing software models will actually be difficult to operate. Existing software models, such as the Waterfall Model, which relies on fully specifying requirements and designing and testing systems, are not aimed at rapid software development. As a result, existing software development models do not provide the necessary products. This is where agile software development leads to remediation. It is specially designed to manage the needs of the rapidly changing environment by accepting the idea of a progressive development and developing the actual end product.

Agility Principles:

1. Our top priority is to satisfy our customers by delivering valuable software increment early and continuously.

2. We welcome changing requirements in the second half of development.

3. Deliver software increment frequently, from two weeks to a few months, with a shorter schedule preference.

4. Building projects on individuals' motivation. Give them the environment and support they need, and trust them to accomplish the job.

5. Working software module is the main measure of progress.

6. The most effective and effective way to communicate information to the development team is through direct conversations.

7. Simplicity Techniques that maximize workload are essential.

2.4.2 Agility and the cost of change

The standard method for considering in programming movement (upheld by various quite a while of experience) is that the gotten of development increments nonlinearly as an endeavor advances (Figure 2.3, strong dull curve). It is adequately essential to oblige an adjust when a thing pack is gathering requirements (on schedule in a meander). A use condition must be changed, a summary of limits likely could be widened, or a made explicit can be changed. The expenses of doing this work are irrelevant, and the time required won't unfavorably affect the consequence of the endeavor. Be that as it may, imagine a circumstance where we quick forward various months. The pack is in the midst of endorsement testing (something that occurs generally late inside the meander), and a fundamental accessory is asking for an imperative reasonable adjust. The modify requires a change to the compositional organize of the thing, the outline, and progression of three present day parts, adjustments to another five portions, the arrangement of unused tests, etc.

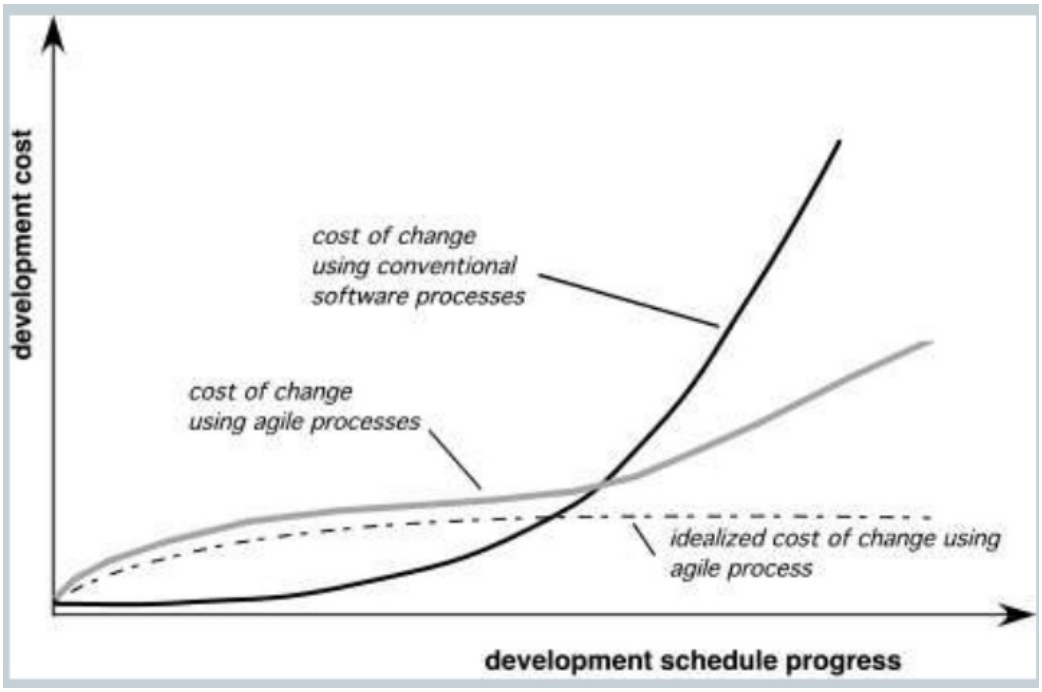


Figure 2.6: Agility and the cost of change

Advantages of Agile Methodology:

- Software increment delivery is faster, which helps increase customer confidence.
- You can better adapt to rapidly changing requirements and respond more quickly to new requirements.
- The following steps will help you get immediate feedback that you can use to improve your software.
- Continued interest in technical excellence and superior design.
- It is not a person-process. Interaction with people is given priority over processes and tools.

2.5 Scrum

Scrum could be a quick structure for organizing work with a feature on the programming development. It is orchestrated social gatherings of three to nine fashioners who break their work into works out that should be possible inside time boxed cycles, called runs (routinely two-weeks) and track advance and re-plot in 15-minute stand-up social endeavors, called well ordered scrums. Approaches to deal with arranging made by differing scrum packs in increasingly significant affiliations set Large-Scale Scrum,Scaled Dexterous System (SAF) and Scrum of Scrums, among others.

Figure 2.7: Scrum design of project

Scrum has three roles: Product Owner, Scrum Master, and Team:

- **Item Owner:** THe said that the owner of the goods, sight, ace, Openness. The Item Proprietor is responsible for the ongoing delivery.Vision and necessity for change. Sometimes The product provider changes the way of thinking that is appropriate. Because I admire Scrum Self-relation between social events, the item provider should counter the necessity. Directly on a liter scale. Potentially, the item owner should have access to:Ask for a reply at a meeting.

- **Scrum Master:**ScrumMaster is a member of the software development team that practices Scrum, the most widely used and widely used software development framework. The main role of ScrumMaster is to help you take responsibility for your team's work responsibilities and eliminate obstacles that can hamper your team's productivity. ScrumMaster aims to help teams focus on their work and align with the appropriate Scrum workflow, while training and motivating them without forcing them. They met with the team regularly and reviewed the work and results, usually at the end of each week. ScrumMaster is an effective team model just like any effective leader. At the same time, ScrumMaster is not a pioneer in traditional management because it does not have the power to dismiss or remove team members.

- **Team:** s described by the Scrum coordinator, "The assembly is completely self-managed." Total progress is capable of self-organization of aggregate action. a The Scrum Movement amass contains about seven fully loyal individuals (officially 3-9), in an ideal world in one pool room guaranteed by external redirection. For learners in programming, regular clustering builds a mix of programming engineers, programming units, software engineers, examiners, quality assurance experts, analysts, and user interface regulators

2.6 Functional Requirements

Functional requirements include registration of the user in the app, adding product to the cart, adding value coin to the wallet, making payment for the product in the cart, Check their balance. See their past transactions, Admin can add products to the shop, Generate bar code for the given product.

2.6.1 Registration of the user in the app

This module takes necessary details like email address,name,phone number,date of birth and password of the user and it will add a user to the blockchain of the customer. Blockchain of a customer is basically a linked list so it stores previous block hash value for making the chain continuous.Nounce will be a random number which is

used for the generation of the hash value of the block.It will provide security to the block.Registration of the user is varified by the admin.

2.6.2 Adding product to the cart

Each product has its bar code associated with it. When we scan the product using the mobile app. the product is automatically added to the cart. Each bar code has eight digit number associated with it. Detail about the product is stored in the database. it will fetch corresponding value and it will add into the cart. Product price is decided by the admin and stored in the database. and admin will generate corresponding bar code and put into the product. When we scan the barcode phone will fetch necessary details from the database and it is added into the cart.

2.6.3 Adding value coin to the wallet

Since all the payment will be done using our made currency ie ValueCoins. We must add money to our application in the wallet provided. It will convert all the currency into ValueCoins as per the rate decided before. for adding value coins to wallet we need information about the number of coins to be added and userid of the customer. It will take this information and send it to the genesis block then genesis block release coins and this coins is added to the user's wallet. The user can use these coins for shopping the product.

2.6.4 Making payment for the product in the cart

After doing all the shopping they can just pay the amount, displaying below the cart. Payment will be made using the ValueCoins present in the wallet. for making payment we need to send total shopping amount and wallet balance and userid of the customer is sent to the server, the server will check the validity of the transaction if the transaction is valid then the transaction is added into the blockchain one copy of transaction is sent to the user and other is stored in the server.if transction is not valid then it is discarded by the server.

2.6.5 Checking Balance of User Wallet

After making all the payment or before shopping customer can check their balance. for checking the balance of user wallet we need to sent request to the server for balance inquiry the server will return the balance of the user and it will be displayed into user wallet.

2.6.6 Display their Previous Transection

It will show the list of transaction made. It will contain only up-to a certain number or a certain time. It will have details of the transaction such as coins spent, products are taken, coins rewarded for shopping. It will show details about a transaction made and their amount and their date is shown to the user.

2.6.7 Change their credentials

If one customer feels like one should change their credentials, they can by just providing certain details which will be available only with the authorized user.User have to provide details to be changed and new value to be replaced is sent to the server and server will update the crossponding value.and reflaced into the app.

2.6.8 Adding Product to the Shop

Admin can add the product to the shop. Admin takes details about the product and adds into the database.based on their value and properties admin will generate a barcode for the product. This barcode is used for adding a product in the cart.

2.6.9 Generation of Barcode for product

While adding product to the cart user will generate barcode for the product.it will take details about product and using barcode generator code it will 8digit number and crossponding barcode is generated.

2.7 Non-Functional requirements

In system engineering and requirements engineering, non-functional requirements are requirements that will ultimately determine the standards It can be used to judge the operation of the system, rather than any specific behavior. They are in complete contrast to the specific functional requirements or behavior or function.

2.7.0.1 Accessiblity

This stage refers to the design of the products, all the devices and services or even the environments for all the people with disabilities. The concept of accessible design ensures both "direct access" and "indirect access" meaning the compatibility with a person's adaptive technology.

2.7.0.2 Configuration Management

Configuration Management is considered as the type of all system and system Maintenance of a product performance stability, function and the same Physical attributes with its requirements, design and operational information It will get a lifetime.

2.7.0.3 Privacy

Privacy will be considered as a personâĂŹs ability or perhaps in some cases a group of people who need some kind of or some kind of security maybe for yourself or maybe even for information about yourself and ultimately express them selectively. The boundaries will obviously be different for each culture.as well as for a person who is considered an enterprise staff, but willshare common themes or agendas.

2.7.0.4 Usability

This is the case when we need ease of use and the study of the ability of a person-created object. In SE (software development), usability is the extent to which software can be used by specified product consumers in order to ultimately achieve ultimate quantitative goals with full efficiency, effectiveness and satisfaction quantitatively so that you can measure everything in the development process and choose the best optimal solution Stages o SDLC product.

2.7.0.5 Availability

This is the extent to which the system will be available or will be present working state or even in a certain specified working and fixed state at the start of the mission, when the mission is requested for an unknown person, i.e. random time To keep it simple and easy for all of us, we can say that availability is the fraction of the time the system is operational.

2.7.0.6 Scalability

This is the ability or function of the system or perhaps the network or maybe even the process that can handle a growing amount of work, or it could its potential to be increased to meet growing growth.

2.7.0.7 Modifiability

This usually speaks of staffing efforts that will be necessary and will be make any changes to the system after some development in the system it would be very difficult if you had to make any changes to later stages of software development, so it would be advisable to perform all kinds of changes and modifications, if necessary in the initial stages.

2.7.1 Reliability

This will about the ability of the system or the ability of a component to function. all in accordance with the stated conditions for certain or certain successive conditions

Chapter 3

Detailed Design

Here we examine the interface plan of the venture. The task is intuitive with the average citizens. We have portrayed the information structure utilized just as for certain calculations that were utilized by our framework.

User Interface Requirements

- The framework should and ought to have the capacity to resemble a graphical UI and not some content based interface like the ones that were found in the absolute starting point phases of the PC ERA, we incline toward such a graphical interface for simple use and comprehension.

  The framework should and should ready to provoke the client for the subsequent stage that will be performed amid the way toward utilizing the framework.

- The framework should likewise have the capacity to show every one of the subtleties and every one of the run-downs when and where required and in no other position.

- The System must ensure that all the unique individual who has their very own records are treated as independent people with various functionalities so that there will be no irregularities and each individual or client might want the framework and might want to utilize the application.

Concept Requirement List (CRL) is or are the arrangement of prerequisites which would show the general framework, it's needs and every one of the yields. These are the arrangement of necessities by and large given by the administration to the planners. Following are the arrangement of CRL for the All in versatile therapeutic administrations.

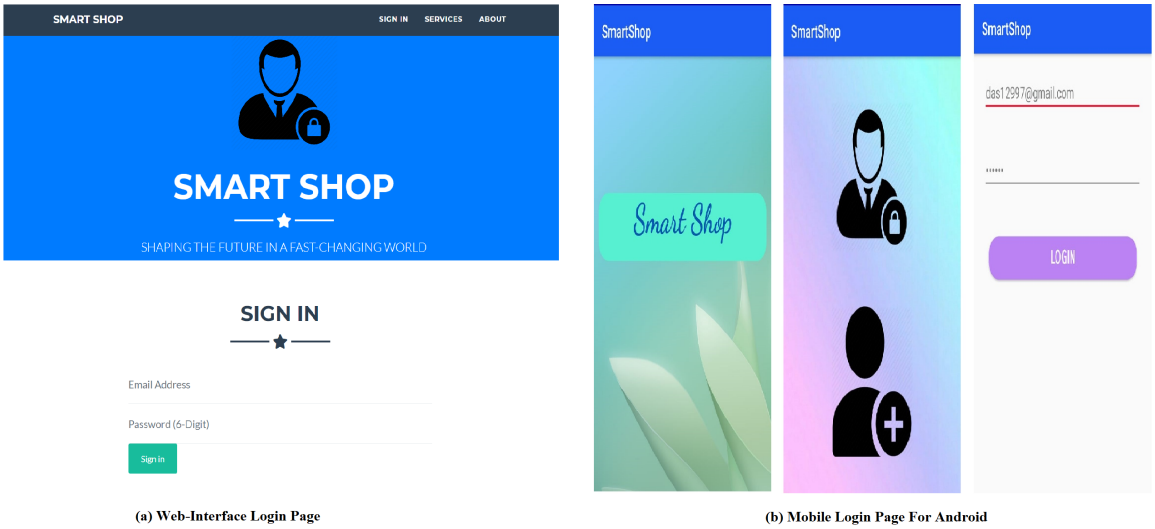
- Framework underpins the most well-known and generally utilized language i.e., English.
- Client ought to have the capacity to enlist himself as a client in the application with no error.
- The client ought to have the capacity to log just into their particular records and not into some other record.
- The framework must help all the important highlights and functionalities.
- The framework ought to have the capacity to show all the accessible basic need things present in the store to the clients.
- All the important data ought to and must be shown in an entrenched way.
- The framework ought to be tough for unpleasant utilization of the application.
- The framework must be a graphical UI (GUI) with the goal that it is anything but difficult to utilize and would likewise be simple for getting purposes.

3.1 Interface design

Here we look into the interface of the system as the interface is the means through which or the medium through which the the user will be able to interact with the system and also be able to access the database for reading and writing a record into the database. So therefore the interface design should be of really good quality, the main thing is to get the best look and feel out of the system.

3.1.1 Login Page Interface Design

The application will open with a login page and a sign up page. New user will have to login into our system and provide all the required details during the signing up. All the details asked will be useful for running our application successfully and reaching the expectation.



(a) Web-Interface Login Page

(b) Mobile Login Page For Android

Figure 3.1: User Interface for both Web and Mobile.

Once sign-up procedure is completed, user have to login again into the system via the application using their credentials. Customers can also change their credentials again afterwards according to their wish and comfort.

3.2 Data Structures and Algorithms

3.2.1 Block Creation

A block is a piece of exchanges in a value-based blockchain. A block could truly contain any sort of data and a chain of these blocks develops into a blockchain as long as it joins one and other. Blockchain is a permanent information structure comprising of a rundown of blocks where each next square contains a hash of the past square. Because of this hashing, the chain of blocks winds up unaltered: you can not change or erase a block from the center of the chain without reconstructing

every one of the blocks above, on the grounds that the smallest change will require a remake (recalculating hashes) of all blocks over the transformed one.

Data Structure Used: A block contains a hash, previous hash value, an array list of transactions to store each and every transaction of the customer and the timestamp of creation of the block.

Use Cases: Every transaction is stored in a block. The customer transaction and data is stored in a block and hence block creation is a mandatory step in process of completion of a transaction.

Algorithm 1 Block Creation

$FirstHash \leftarrow 0$
$timestamp \leftarrow Date().getTime()$
$CurrentHash \leftarrow generateHashUsingSHA256(previousHash + timeStamp)$
$PreviousHash \leftarrow PreviousHash$
if $ProcessTransaction \neq true$ **then**
  $TransactionFailed!$
else
  $AddTransactiontoBlock!$
end if

Error handling: Validate authenticity of transaction using previousHash value. If previousHash value of new transaction is not valid then the transaction is false and should not be accepted. This condition is checked using the if construct.

3.2.2 Construction of E-Wallet

Blockchain wallet is a PC program that permits to screen and direct cryptographic money. It is an advanced wallet that enables clients to oversee bitcoin and ether.E-wallets enable people to store cryptographic forms of money. On account of Blockchain Wallet, clients can deal with their equalizations of cryptographic forms of money: Value-Coins. The Blockchain Wallet interface demonstrates the present wallet balance.

Data Structures used: The e-wallet consists of a USerID, private key, public key and a hash map of Unspent Transaction Outputs (UTXO). Use Cases: The wallet contains public and private key for the client security and a HashMap for mapping exchanges alongside intends to send assets to the retailer for the buy.

Algorithm 2 EWallet Construction

$UserID \leftarrow email$
call GenerateKeyPair()
$PrivateKey \leftarrow getPrivateKey()$
$PublicKey \leftarrow getPublicKey()$
$PreviousHash \leftarrow PreviousHash$
if $WalletBallance < TransactionValue$ **then**
  $TransactionFailed : InsufficientBalance!$
else
  $Transactionsuccessful!$
  $GenerateSignature$
end if

Error handling: The False transactions are checked for using the concept of Unspent Transaction Outputs.

3.2.3 Block Creation

A block is a piece of exchanges in a value-based blockchain. A block could truly contain any sort of data and a chain of these blocks develops into a blockchain as long as it joins one and other. Blockchain is an interminable data structure involving a once-over of squares where each next block contains a hash of the past block. In light of this hashing, the chain of blocks ends up unaltered: you can not change or delete a block from the focal point of the chain without reproducing all of the blocks above, because the littlest change will require a revamp (recalculating hashes) of all block over the changed one.

Data Structure Used: A block contains a hash, previous hash value, an array list of transactions to store each and every transaction of the customer and the timestamp of creation of the block.

Use Cases: Every transaction is stored in a block. The customer transaction and data is stored in a block and hence block creation is a mandatory step in process of completion of a transaction.

Error handling: Validate authenticity of transaction using previousHash value. If previousHash value of new transaction is not valid then the transaction is false and should not be accepted. This condition is checked using the if construct.

Algorithm 3 Block Creation

$FirstHash \leftarrow 0$
$timestamp \leftarrow Date().getTime()$
$CurrentHash \leftarrow generateHashUsingSHA256(previousHash + timeStamp)$
$PreviousHash \leftarrow PreviousHash$
if $ProcessTransaction \neq true$ **then**
  $TransactionFailed!$
else
  $AddTransactiontoBlock!$
end if

3.2.4 UTXO

In the blockchain data structure of a location "containing coins,""coins" are really put away as "unspent exchange yields" or UTXOs for short. A UTXO can be related with a crypto-coin address, however, you can likewise have a wide range of UTXOs that are related with the equivalent crypto-coin address. The "address balance" is the total of the majority of the estimations of UTXOs related to the address. The unspent exchange yield show connected in blockchain is a more conceptual idea that the record based model utilized in blockchain. It is an essential part of blockchain that considers the blockchain to be straight through the majority of the exchanges being connected by a chain of the digital signature.

UTXO set is a subset of crypto-coin exchange yields that have not been spent at the given minute. At whatever point another exchange is made, UTXOs are utilized to guarantee the assets they are holding, and new UTXOs are made. Fundamentally, exchanges expend UTXO (in their data sources) and create new ones. In this way exchanges produce changes in the UTXO set. Since the UTXO set contains every unspent yield, it stores all the expected data to approve another exchange without examining the full blockchain. This concept is clearly illustrated in figure 3.2.

Data Structures used: UTXOs are stored in key-value pair form, wherein if there are several UTXOs belonging to the same payment then are categorised under one key itself.

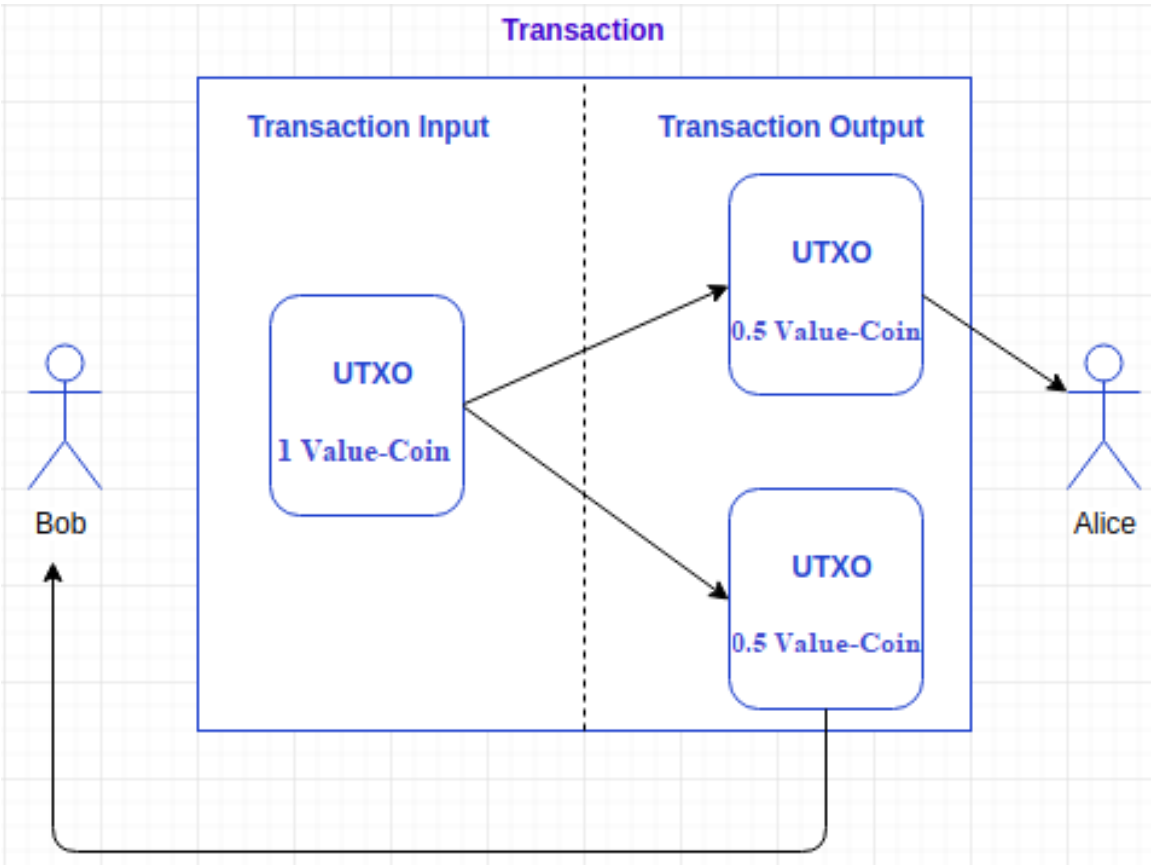


Figure 3.2: Illustration of UTXO transactions

Use Cases: UTXO is an output of the blockchain transaction that has not been spent which is used as an input in a new transaction.

Error handling: The False transactions are checked for using the concept of Unspent Transaction Outputs.

3.2.5 ECDSA Algorithm

The ECDSA is an open key encryption framework which works along these lines to RSA calculation however furnishes more noteworthy security with lesser key size

Algorithm 4 UTXO Updation

Amount ← Value-Coins that are sent to recipient
$SENDERID$ ← unique identifier of the sender
$RECIPENTID$ ← id of the receiver of Value-Coins
Output ← updated sender and receiver wallet balance
if $SenderBallance < Amount$ **then**
  $Declinetransaction : InsufficientBalance$!
else
  commit the Transaction and update the balance of sender and receiver
  $SENDERBALANCE = SENDERBALANCEAMOUNT$
  $RECIVERBALANCE = RECIVERBALANCE + AMOUNT$
  ADD Transaction in the blockchain
end if

contrasted with RSA. The inconvenience of this framework is the likelihood of blunder which makes it conceivable to choose a private key esteem with the end goal that indistinguishable marks for various archives can be acquired. Nonetheless, huge computational execution is required for this opportunity to appear.

Use case: ECDSA is used to generate public and private key of the user for creating a secure transaction.

Algorithm: ECDSA algorithm

ECDSA algorithm involves the following steps:

(i) Setup

1. The elliptic curve group $E(a, b, p)$ with parameters a, b, p, and order either prime n or divisible by prime n
2. The primitive element $P \in E$, which is of order n
3. The prime p which is of 160 bits or more
4. The private key which is a random integer $d \in [2, n2]$
5. The public key which is a point on the curve $Q = [d]P$

(ii) Signing

1. Generate a random integer $r \in [2, n2]$
2. Compute $[r]P = (x_1, y_1)$
3. Compute the integer $s_1 = x_1 \, (mod \, n)$
4. If $s_1 = 0$, stop and go to Step 1
5. Compute $r^{-1} \, (mod \, n)$
6. Compute $s_2 = r^{-1}(H(m) + d * s_1) \, (mod \, n)$
7. If $s_2 = 0$, stop and go to Step 1
8. The signature on the message m is the pair of integers (s_1, s_2)

(iii) Verification

1.The verifier receives the message and the signature: $[m, s_1, s_2]$
2. The verifier knows the system parameters and the public key Q
3. The integers s_1, s_2 are in the range $[1, n1]$
4. Compute $w = {s_2}^{-1} (mod \, n)$
5. Compute $u_1 = H(m) * w \, (mod \, n)$
6. Compute $u_2 = s_1 * w (mod \, n)$
7. Compute $[u_1]P \oplus [u_2]Q = (x_2, y_2)$
8. Compute the integer $v = x_2 \, (mod \, n)$
9. The signature is valid if $v = s_1$

3.2.6 SHA-256

We utilize the BouncyCastle library to perform essential cryptographic activities, for example, encryption and mark. BouncyCastle is a Java library that supplements the default Java Cryptographic Extension (JCE).

In a genuine circumstance, we frequently need to sign at that point scramble our information, that way, just the beneficiary can decode it utilizing the private key, and check its credibility dependent on the advanced mark. With BouncyCastle we can create a computerized declaration and a private key which are for the most part utilized in awry cryptographic tasks:

- Encryption
- Decryption
- Signature
- Verification

The beneficiary is bound to a declaration, that is freely shared between all senders.

Basically, the sender needs the beneficiary's declaration to encode a message, while the beneficiary needs the related private key to have the capacity to decode it. The encryptor is utilized later to create an information object that exemplifies the scrambled message.

At long last, the encoded portrayal of the envelope is returned as a byte exhibit. The beneficiary gets the decoded/typified message, which we can't recover except if we have the comparing beneficiary's critical.

At long last, given the beneficiary key as a contention, we return the crude byte exhibit separated from the Enveloped Data to the related beneficiary.

Hash capacities are utilized to give information uprightness and are utilized along with advanced mark calculations and MACs to additionally give verification. Out of the many essential hash work of the SHA breed, which share the equivalent useful skeleton with some variety in the inner tasks, message estimate, block size of the message, word estimate, number of security bits what's more, message hash measure.

These calculations are iterative and single direction capacities that take as input a message and yield a message digest. They process the info information into

two phases: preprocessing and digest calculations. The preprocessing guarantees that the message has a size that is various of a specific esteem, permitting to partition the message into predefined blocks sizes and to give an underlying hash esteem.

In the second round, each message block is utilized in the midst of a fixed number of accentuation, where every cycle describes limits, constants and word exercises to create a movement of hash regards. Once all, blocks are handled, the estimation of the last hash is utilized as the message digest. Specifically, the second phase of the SHA-256 calculation performs 64 emphasizes over blocks of 512-piece messages and hash estimations of 256 bitsa s 8 32-bit words (A, B, . . . , H). The hash message is 256 bits in length.

Data Structure Used: Array and hash map

Use Case: To verify authenticity of customer transactions using secure digital signature method.

Algorithm 5 SHA-256

for $i \leftarrow 1$ to N
Prepare the Message Schedule W.
Initialise the eight working variables A,...,H
for $i \leftarrow 0$ to 63:
    Calculate Temporal Temp1
    Calculate Temporal Temp2
    Calculate Temporal H, G, F
    Calculate E = D + Temp
    Calculate new D, C, B
    Calculate new A=Temp1+Temp2
Compute i^{th} intermediate hash value H^i.
Generate Message Digest with H^N.

3.2.7 Attribute Based Encryption

Attribute-based encryption (ABE) is a moderately late methodology that re-evaluates the idea of open key cryptography. In customary open key cryptography, a message is scrambled for a particular recipient utilizing the collector's open key. Character-based cryptography and specifically personality based encryption (IBE) changed the customary comprehension of open key cryptography by enabling the open key to be

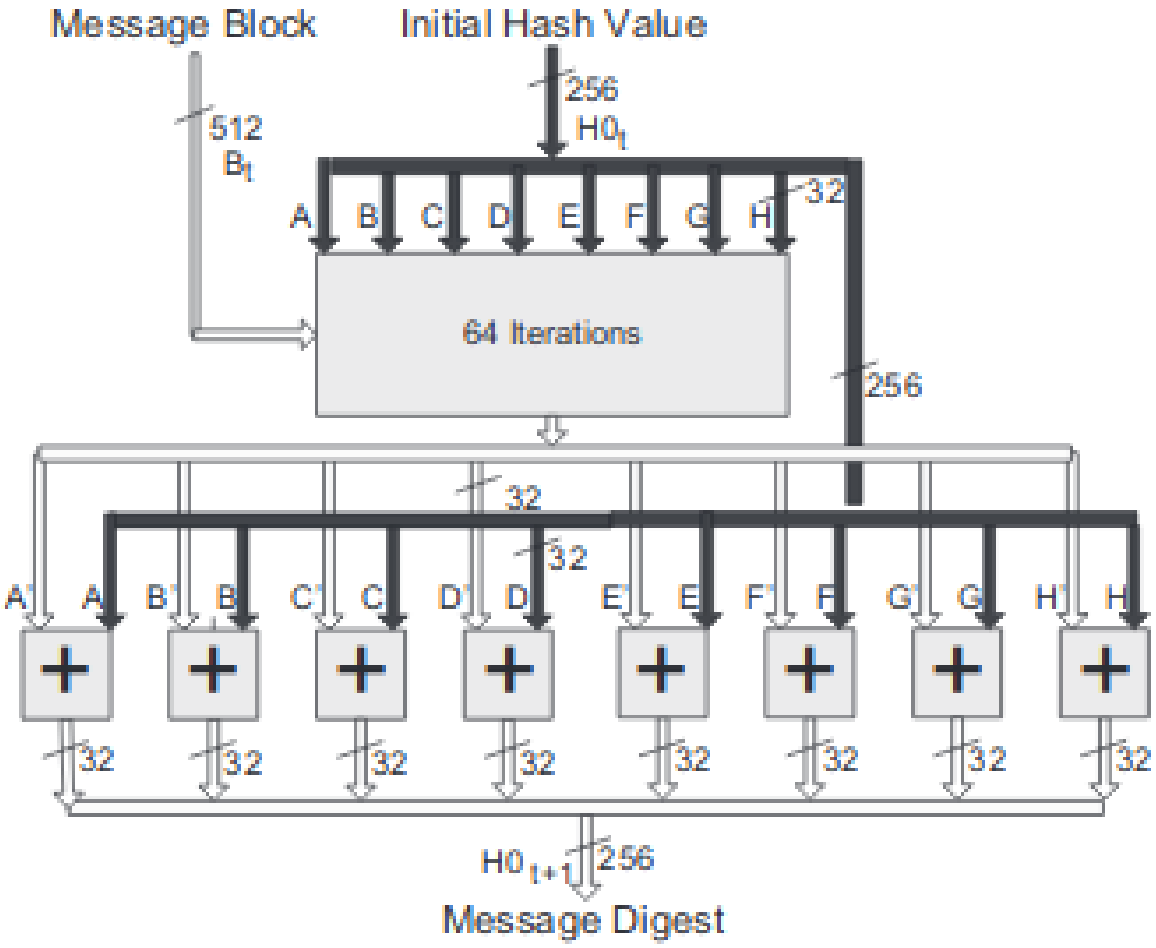


Figure 3.3: SHA-256

a self-assertive string, e.g., the email address of the collector. ABE goes above and beyond and characterizes the personality not nuclear but rather as a lot of properties, e.g., jobs, and messages can be encoded as for subsets of characteristics (key strategy ABE - KP-ABE) or strategies characterized over a lot of traits (cipher text-arrangement ABE - CP-ABE). The key issue is, that somebody should possibly have the capacity to decode a cipher text if the individual holds a key for "coordinating qualities" (more underneath) where client keys are constantly issued by some confided in gathering.

Cipher text Policy- ABE

In an encrypted content-arrangement quality constructed encryption (CP-ABE)a customer's private-key is connected with a great deal of attributes and a figure content demonstrates a passageway system over a portrayed universe of properties inside the structure. A customer will be able to unscramble a figure content, if and just if his attributes full fill the methodology of the individual cipher text. Arrangements can be described over characteristics employing intersections, unions and (k,n)- limit doors. i.e. k out of n, features must be obtainable. For example, let us suppose that the realm of features is with holding the features (A,B,C,D)and customer 1 obtains a secret route to properties (A,B) as well as customer 2 to quality (D). On the off chance for a cipher text to be scrambled regarding the method $(A \wedge C) \vee D$ provokes customer 2 to certainly decode, while customer 1 won't probably unscramble. CP-ABE in this way allows to validate understood permission, i.e., permission is added into the scrambled refined data and only those people full filling the related arrangement can unscramble information. One more decent component is customers can get their private keys once the information has got enciphered relevant to the strategies.Hence the refined data is enciphered without learning about the common permutation of customers which will most likely unscramble by denoting the strategy which enables decoding. The probable tentative customers who can be awarded a key regarding characteristics with the end goal which the arrangement can be completed will at that point have the ability to decipher the refined data in an encryption system based on cipher text policy attributes, the customer's private key is related to a collection of features (describe the customer), and the encoded cipher content will over-allocate the specified access policy. The customer is permissible to decrypt if it with holds the cipher text policy.ABE is an encoding component that is helpful in settings where the list of clients may not be known a priori, however all clients may have certain accreditations which can be utilized in determining access control and in the meantime giving a sensible level of namelessness. Cipher text policy quality based encryption is a plan that gives a characteristic method to interface the entrance arrangement with the cipher text, and properties with the keys; and keenly join them at a later stage to give secure access to ensured information.

A cipher text-arrangement characteristic based encryption conspire comprises of four key algorithms: Setup, encode KeyGen and Decrypt. Moreover, the choice of a fifth calculation Delegate is taken into consideration.

Use-Cases: The Attribute Based Encryption is implemented in the file level to protect the cipher text based encrypted user data.

The algorithm proceeds in the following manner:

1. **Set up** :This random calculation takes as information the certain security parameter and a couple of framework parameters (d, num). This parameter will be utilized to limit the entrance trees under which messages can be encoded in our framework. It yields the public parameters(PK) and a master key(MK).

2. **Key Generation(M,K,S)** ::The calculation of the key takes into account the master key MK and a lot of attributes that portray the key. It yields a private key or decryption key SK.

3. **Encrypt(PK,M,A)** ::The encrypted calculation accepts as info the open arguments PK, a message M, and an access structure. The calculation scrambles and delivers a cipher text CT with the objective that just a customer who possesses a lot of qualities that full fills the entry framework will probably decode the message. We can assume that the cipher content certainly consists get to structure A.

4. **Decrypt(PK,CT,SK)** : The unscrambling calculation takes as information the open parameters PK, a cipher text CT, which contains an entrance approach A, and a private key SK, which is a private key for a set S of properties. In the event that the set S of properties full fills the entrance structure At hen the calculation will unscramble the cipher text and return a message M.

5. **Delegate(SK,S)** : The representative calculation takes as information a mystery key SK for some arrangement of traits S and a set ($S \subseteq S$). It yield a mystery key SK for the arrangement of traits S.

3.2.8 Consensus Mechanism

The accord calculation assesses the criterion's and conditions that are to be come to so as to approve the obstructs that are to be incorporated into the blockchain. The agreement calculation is a result of the Byzantine Generals' Problem which expresses that any two gadgets on the decentralized temperamental system can't totally and unquestionably find out that they are speaking to similar information. The Byzantine Fault Tolerance is a characteristic which signifies the extreme arrangement of blemished hubs that are related with the Byzantine Generals' Problem. It can endure up to thirty-three percent flawed hubs that are 3f+1 where f is the all out number of defective copies present in the framework. Essentially, there are four confirmations used to execute the agreement calculation: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Proof of Authority (PoA).

The blockchain hub arrange overseers are in charge of following administration brought forth works :

- Assigning and holding jobs/consents that are utilized to approve hub movement to trusted and fit members.
- Securing open and private keys for confirmation and approval purposes.
- Encrypting information by means of founded cryptography rehearses.
- Storing decides that speak to savvy contracts, and for the conjuring of these.
- Formulating and establishing accord approval algorithm(s)
- Maintaining a hub's handling history, and its level of achievement.
- Recording of administration level understandings (for example execution, uptime), as affirmed by the hub organize overseers.
- Managing and checking of system execution by balancing the heap among the hubs, detecting maverick dangers and vindictive action,monitoring the machine condition of the system and evaluating a hub's handling exhibition against any administration level understanding estimations.

Table 3.1: Comparison of various Consensus Algorithms

	PoW	PoS	DPoS	PoA
Principle	The arrangement is unpredictable to find however helpful to approve.	The arrangement is unpredictable to derive however advantageous to approve.	Board of representatives chosen by clients of the system screen the blockchain and propose changes to the convention which must be affirmed by the clients.	Blocks are approved whenever marked by a predefined majority of endorsers.
Node Recognition and Administration	Open	Open	Open	Permissioned
Energy Saving	No	Partial	Partial	Yes
Tolerated Power of Adversary	Below 25 percent computing power	Below 51 percent stake	Below 51 percent validators	Below 33.33 percent validators
Throughput	Below 100	Below 1000	Below 1000	Below 2000
Scalability	Strong	Strong	Strong	Weak

Since the proposed framework utilizes a private blockchain it is good to actualize PoA organize for keeping up the accord. PoA is a substitute for PoW in private blockchains which comprises of specialists hubs who are in charge of manifestations of a square and secure activity and support of bockchain. Two primary calculations

used to execute PoA is AuRa and Clique. PoA comprises of N confided in specialists wherein at any rate N/2+1 experts should deliver a similar outcome in the wake of leading their activity to look after agreement.

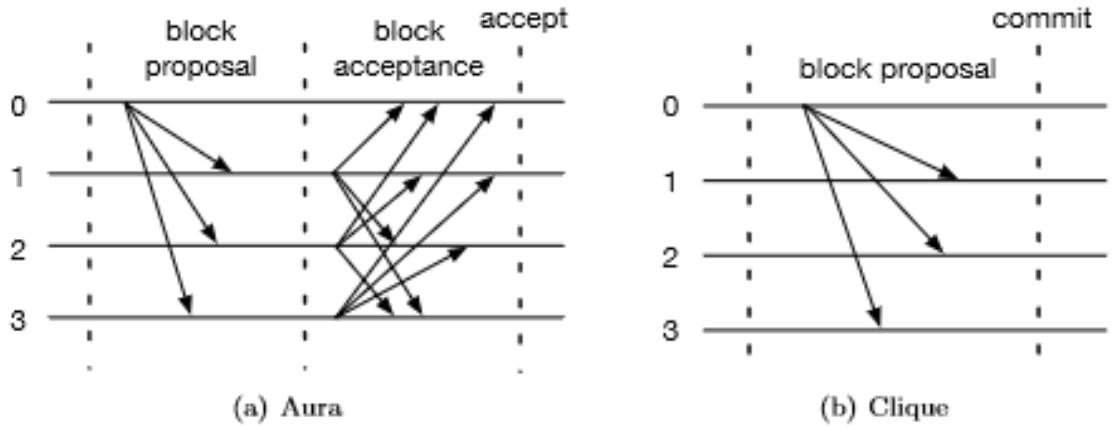


Figure 3.4: Message trades of Aura and Clique PoA for each progression. In this model, there are 4 experts with id 0,1,2,3. The pioneer of the progression is specialist 0.

AuRa is implemented in Kovan network. It contains three criterion's: check of hubs (n), the total of broken hubs (f) and division of time term (t) called ventures right away. The time length for each progression is chosen deterministically by the equation $UNIXTIME/t$ where t is some consistent used to partition the time made for each stride in a discrete way. In AuRa each block is acknowledged in two rounds. Toward the start of the first round, the pioneer is chosen by id mod n where id is a counter initialised to zero increased by one each time there is a solicitation for square creation. In the first round, the pioneer communicates the proposed square to the various specialists. In the second round, the block is acknowledged just if N/2+1 experts guarantee to have gotten a similar square. In this plan, the pioneer is viewed as malevolent when most of the specialists don't have trust in the pioneer. This circumstance emerges when the pioneer does not propose a block or the pioneer proposes a greater number of squares than anticipated or if the pioneer has proposed.

Clique is implemented in Geth. It takes just a solitary round to acknowledge a block. In contrast to AuRa, a block can be proposed by the present head just as

other confided in experts. Be that as it may, the block proposed by the present chief is relegated a score of 2 while the block recommended by some other real expert is allocated a score of 1. This is done as such that the block proposed by the pioneer has achieved all the marking experts first. A marking specialist can propose a block after ever N/2+1 turn. This keeps a solitary block from proposing a lion's share of the block.

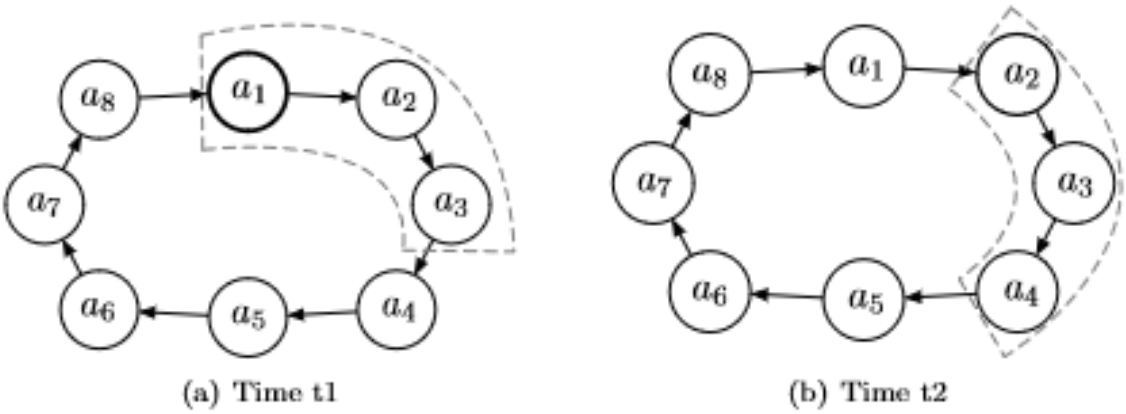


Figure 3.5: Selection of participants enabled to suggest blocks in Clique.

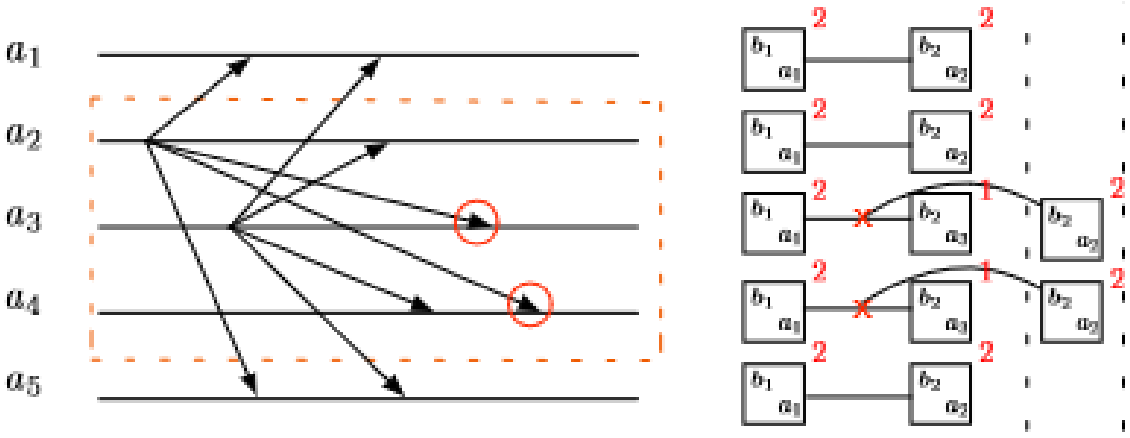


Figure 3.6: A fork happening in Clique.

In the figure 3.6 expert a_4 has the square proposed by a_3 as the second square, while a_5 has the block proposed by a_2. In the long run, a_4 replaces the block proposed

by a_3 with that proposed by a_2 in light of the fact that the last has a higher score.

3.3 UML diagrams with discussions

3.3.1 Data Flow Diagrams (DFDs)

The DFD otherwise called an air pocket outline is a directly sensible formalism that can be used to address a structure in the terms of the data to the system, diverse planning did on this data, and the yield data delivered by the system. A DFD display utilizes an astoundingly fated number of unpleasant pictures to address the points of confinement performed by a framework and the information stream among these cut-off points. The major inspiration driving why the DFD technique is so acclaimed is likely an immediate after effect of the manner in which that DFD is an amazingly fundamental formalism. It is anything but difficult to grasp and use.

- **Level 0 DFD**

  Now and again, it is called as a Context Diagram. It images the look as though you are investigating a framework via a helicopter. It is an important summary constituting the entire framework. It demonstrates the framework as a solitary abnormal state process, alongside its relationship to the outside agents. It is effectively understood and interpreted by a Layman.

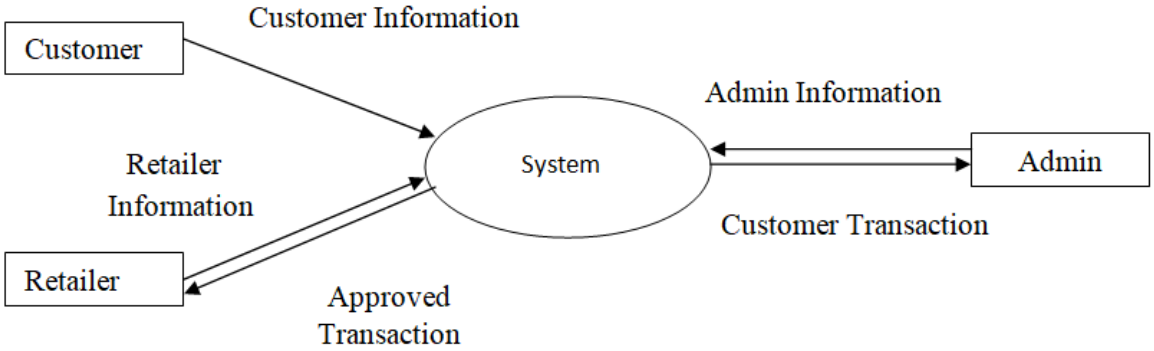


Figure 3.7: Level 0 DFD.

A DFD level 0 diagram consists of only the essential input and the essential outcome. In the current scenario, transaction related information of the

Customer is fed as input into the system. The information pertaining to the retailer and the administrator is also taken as an input into the system. The system processes the transaction informations and sends the output to the administrator. The approved transactions of the customer are forwarded to the retailer.

- **Level 1 DFD**

  It gives an increasingly distinct point of view of the Context Level Diagram. Here, the essential limits did by the system are highlighted as we break into its sub-forms. A dimension 1 information stream format (DFD) is more point by point than a dimension 0 DFD yet not as isolated as a dimension 2 DFD. It confines the fundamental strategies into sub-outlines that would then have the ability to be dissected and improved an increasingly agreeable dimension.

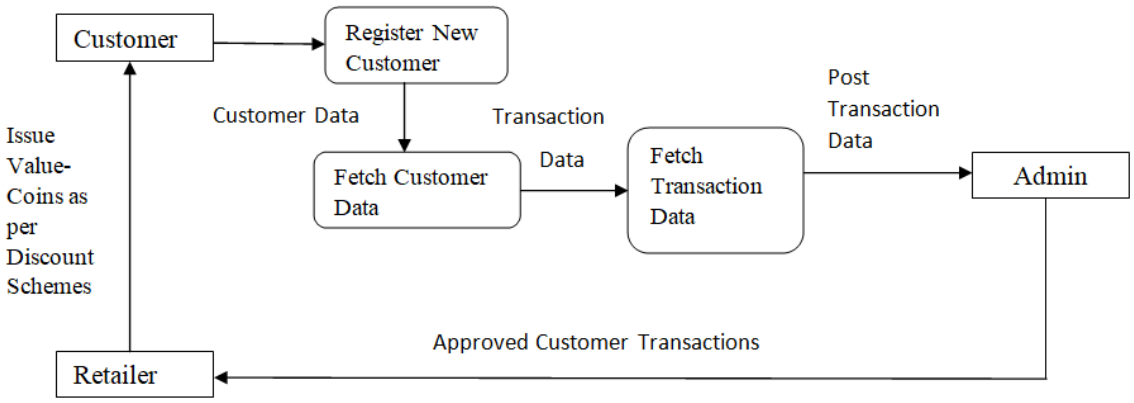


Figure 3.8: Level 1 DFD.

DFD Level 1 diagram contains basically three modules demonstrating three noteworthy executions happening during the time spent leading to a fruitful transaction. First a customer who is using the application for the first time is asked to Register as a New Customer. Then the customer data is fetched in the Fetch Customer Data Module. The relevant transaction details of the customer is extracted and fed into the Fetch Transaction Data module. From here the transaction details are sent to the administrator for transaction approval. The

approved transactions are sent to the retailer. The retailer issues the Value-Coins for the customer as per the discount schemes. This terminates the process of a successful transaction.

- **Level 2 DFD**

  Level 2 DFD goes one phase further into parts of Level 1 DFD. This dimension of DFD may require increasingly substance to accomplish the basic dimension of knowledge about the working of the system. A level 2 data stream diagram (DFD) offers an increasingly positive take a gander at the systems that make up a data structure than a dimension 1 DFD does. It tends to be utilized to plan or record the particular excellence care results of a structure.

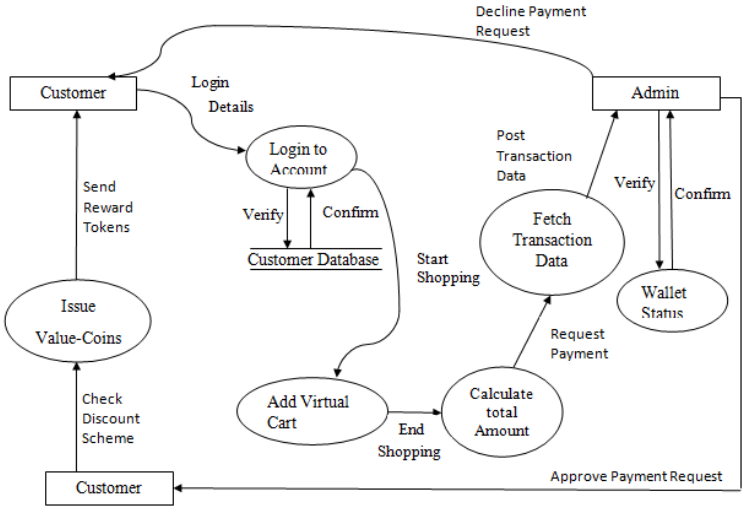


Figure 3.9: Level 2 DFD.

3.3.2 Use Case Diagrams

A utilization chart diagram at its most clear is a delineation of a client's planned exertion with the framework that displays the relationship between the client and the specific use cases in which the client is consolidated. An utilization case graph can perceive the different sorts of clients of a structure and the specific use cases and will a great part of the time be joined by different sorts of diagrams also.

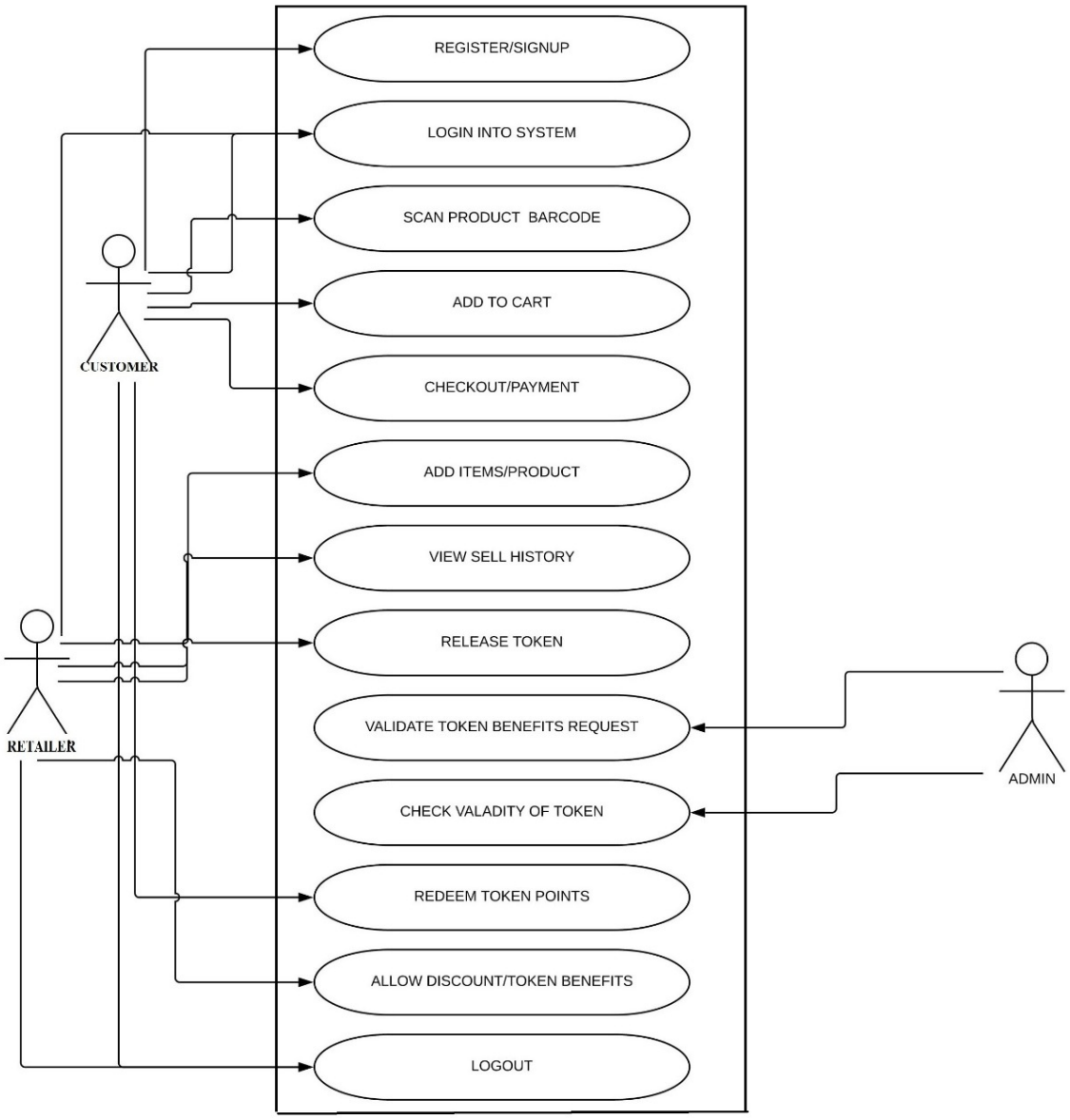


Figure 3.10: Overall Use Case Diagram.

The use case diagram here clearly illustrates the various operations than can be performed by the three users present interacting with the system namely: customer, retailer and administrator. The customer is prompted to new User Registration Page if the user is using the application for the first time. Otherwise, the user is taken to sign-up page to enter their credentials and shop smoothly. A virtual cart is provided

to the customer on successful sign-up where in the customer can choose the item to be purchased, scan the product bar code and add it to their cart. After adding all necessary products into the cart the customer can go ahead with the confirm payment option.

The administrator is the one who validate the users request to make payment. It checks for the customers existing wallet details to approve the payment. On successful validation by the administrator the transaction is forwarded to the retailer. The Retailer can now issue Value-Coins to the customer on the basis of the existing Discount Schemes. Apart from this the retailer is also entitled to add products into the store, view their sell history and logout.

3.3.3 Sequence Diagram

The sequence diagrams are those charts that would give a graphical portrayal to how an assignment is to be practised by passing a succession of messages among the articles. These communications essentially demonstrate the execution and conduct of the on-screen characters included or that are related together and that would in the end cooperate together to play out a few or the other kind of errand or capacity that has been recognized by the framework.

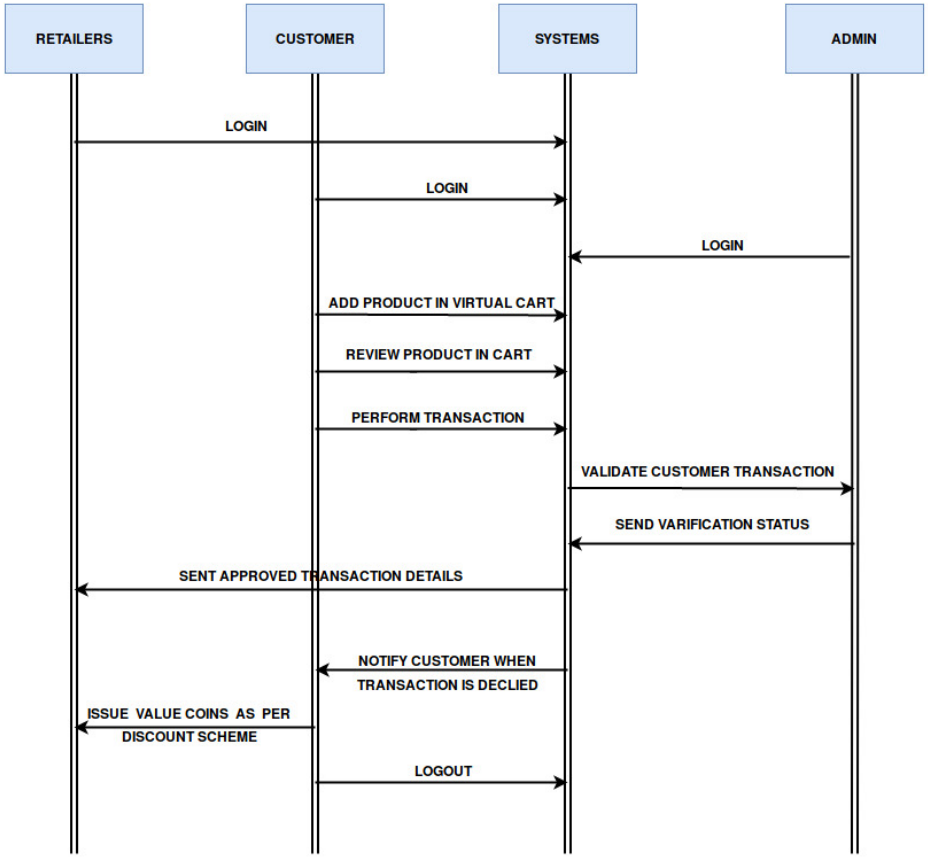


Figure 3.11: Overall Sequence Diagram.

Here in this sequence diagram we become more acquainted with that every one of the on-screen characters present in our framework are altogether required to make the framework an effective one. The actions performed by them have been described sequentially.

Initially, all the three actors: customer, retailer and the administrator log into the system. The user then adds items to the virtual cart provided by the system. On completion of the shopping the customer reviews the items added to the virtual cart and then clicks on the confirm payment button to perform the transaction. Here is where the Administrator comes into the picture next. The administrator verifies the customer's existing e-wallet status to approve the transaction upon receiving the request for customer transaction validation by the system. The administrator then sends the transaction verification status to the system. The system forwards only the approved transactions of the customers to the retailer. The Retailer can now issue Value-Coins to the customer on the basis of the existing Discount Schemes. These tokens are then forwarded to the system. The system then forwards these issued Value-Coins to the customer. This completes the entire process of transaction. After which the customer logs out of the system.

Chapter 4

Implementation

4.1 Tools and Technalogy

4.1.1 JSP(Java Server Pages)

Java-server pages were discharged in 1999 by Sun Microsystems. Jsp is an innovation that will assist engineers with creating dynamic produced site pages. It will utilize java programming language, for the reason. The web compartment makes JSP certain things like response, sessi0n, request, applicati0n, page, cong, page C0ntext, out and exception. In the midst of understanding stage JSP engine will make these articles.

4.1.2 SQL

SQL (Structured Query Language) is a database tongue, which is used for actualizing the set away Relational Database Management System(RDBMS) data additionally as handling the stream data. It's signicant influence over precursors is getting to numerous records with single SQL command.SQL was created by the IBM .SQL transforms into the ANSI standard in 1986 and ISO standard in 1987.SQL gives a basic strategy to request the database for any substance. Moreover it gave a straightforward and convincing way to deal with store and manage the data especially meta-data and certications. It gave a cognizant separate unit of limit on a comparable structure.

4.1.3 Database

4.1.3.1 MySql

MySQL is a social database organization system(RDBMS). It was rst released in May, 1995. MySQL was made by the MySQL AB, a Swedish association. Also, now, MySQL is guaranteed by Oracle Corporation. MySQL is an open source programming whose source code is available under GNU General Public License and moreover under dierent restrictive understandings. MySQL comes inopen source MySQL Community Server and the prohibitive Enterprise Server.

4.1.3.2 JDBC

JDBC is an abbreviation of Java Database Connectivity. It is an application programming interface for the Java. It chooses the strategy for database access by the client. It is the bit of Java SE. It gives the best way to deal with social database to address and revive data to it. A JDBC-to-ODBC interface engages relationship with any ODBC-open data source in JVM.

4.1.4 IDE

4.1.4.1 NetBeans

NetBeans IDE is the specialist IDE for Java 8.It gives its code analyzers, converters and editors. Despite Java, it supports PHP, HTML, C, C++, etc. It is an IDE which is open-source. It supports the headway of a wide scope of the Java application improvement.NetBeans IDE can be reached out to an outsider engineer.

4.2 Experemantal Setup

This task advancement required a broadly useful PC/Laptop. The equipment congurations for the framework are:

- Hard disk:- Minimum 500 GB HDD
- Processor:- Intel core i3/i5 processor @2.2GHz

- OS:- Win 8.1/10
- RAM:- Minimum 4 GB

Programming setup subtle elements are:

- Installing JDK, JRE for Java application improvement.
- Installing Eclipse IDE for Java application improvement.
- Installing MySQL for relational database management.
- Setting up environment variable for each required application of the framework for legitimate execution of utilization.

4.3 Coding Standerd Followed

Coding models are basic and further progressively known by coding conventions or programming styles. These are set of precepts and standards which an architect is depended upon to take after while any application improvement. A segment of the principles are clearly being taken after where some are less take after finished. It is a signficant major in keeping up the consistency and the consistency in the source code. It impression can be no doubt on the taking care of programming. Coding shows are a lot of tips for a specific programming language that propose programming style, practices, and techniques for every component of a product written in that language. those shows more often than not cover le business endeavor, space, remarks, announcements, proclamations, white zone, naming shows, programming works on, programming standards, programming guidelines of thumb, design ne rehearses, and numerous others. those are proposals for programming program auxiliary rst-class. programming developers are especially urged to watch those tips to help improve the intelligibility in their supply code and make programming upkeep less convoluted. Coding shows are best appropriate to the human maintainers and friend commentators of a product venture. Shows can be formalized in a recorded arrangement of guidelines that an entire gathering or business undertaking pursues, or might be as

easygoing as the repetitive coding practices of a person. Coding shows aren't implemented by compilers. The two noteworthy kinds of coding principles are as per the following:

- Programming tongue coding standards: Standards what the programming vernacular designers recommend all product engineers should take after.
- Organization coding measures: rules what engineers are depended upon to take after inside the association. There are associations that solitary program in one vernacular where as there are a couple of associations which make programming in a combination of tongues, they normally plan their own specific coding standard.

From the recently referenced coding models, this endeavor takes after the Coding benchmarks created for a programming vernacular. A bit of the endorsed methodology of programming lingo checks are:

- Declaring variables with correct name
- Preserving Indentati0n.
- Naming is associated to its functionality and entity related.

Every Java source le contains a solitary open class or interface. At the point when private classes and interfaces are related with an open class, you can place them in a similar source le as the open class. The open class ought to be the rst class or interface in the le. Java source have the accompanying requesting:

- Package and 1mport statements
- Class and 1nterface declarati0ns

4.4 Functional Implementation

4.4.1 Register/Signup

This is the elementary step for the woking of the project this function is for the costumer to register it self with a unique id and password so that only a authorise

person is given access to the account. This function is used to retrieve the new data and store that data to the block of blockchain.

4.4.2 Scan Product Barcode

This function is provided to the costumer in the android app to scan the product and get the details of the product so the the costumer add that product to his cart and can directly pay from the app. this function helps us to reach the goal of counterless system in which the customer will not have to wait in long queue to checkout the item which he wants.

4.4.3 Checkout/Payment

This function collects the the cost of the cart and validate the transaction in the block before the payment is successful and update the transection in the block(after verification).

4.4.4 View sell history

All the transactions are stored in the block after they are verified using POA . These stored transactions can be retrieved to get the sell history of the customer.

4.4.5 Release Token

The genesis block is responsible for releasing the token ,for initial initialisation of the wallet 100 value coins is been credited into the costumer wallet in our project(as we need to have some initial value).then the concept of UTXO is used for further transaction.

4.4.6 Checking validity of token

The token(value coins) validity is done through the concept of POA. some authorised nodes are present in the blockchain which are responsible for the validation of the transaction if more then 50% of the member agreed that the transaction is valid then the transaction is validated.

Chapter 5

Testing

Testing is a basic stage in the improvement life cycle of the thing; this is the place the bumble remaining from all of the stages are identified. Thus testing has out an incredibly essential impact for quality confirmation and ensuring the unfaltering nature of the item. Amidst, the testing the program to be endeavored is executed with a game-plan of examinations and the yield of the executed program for the investigations are assessed to choose if the program is executing not out of the blue. Missteps were found and remedied by using the going with testing steps and changes are recorded for further occasions. Next, a movement of testing is performed on the system until it is prepared for use.

5.1 Test workflow

5.1.1 Unit Testing

Unit testing puts together affirmation effort with respect to the littlest unit of programming plot-the thing area or module (as showed up in Figure 5.1). Utilizing the part level design depiction as a guide, fundamental control ways are endeavored to reveal messes up inside the limit of the module.

The relative multifaceted nature of tests and the blunders those tests reveal is restricted by the compelled degree set up for unit testing. The unit test bases on the interior preparing strategy for thinking and information structures inside the limits of a bit. This sort of testing can be driven in parallel for different parts.

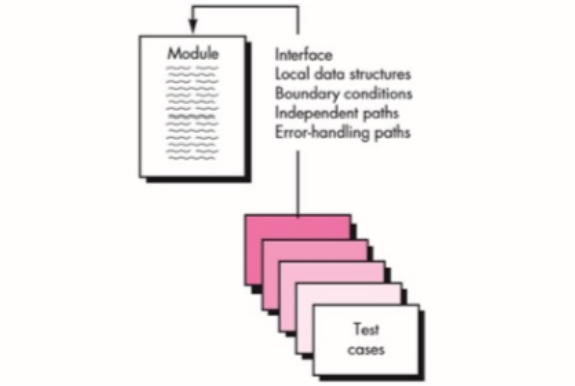


Figure 5.1: Unit Testing

5.1.2 Integration Testing

Integration testing (now and again called blend and testing, truncated) is the phase in programming testing in which solitary programming modules are joined and attempted as a social affair. It occurs after unit testing and before approval testing. The modules that have been unit tested integration testing takes those modules as input and group them in a larger total, and conveys as it yields the incorporated framework prepared for framework testing. It is a proficient system for building up the item programming designing while meanwhile driving tests to uncover botches related to interfacing. The objective is to take unit-attempted sections and create a

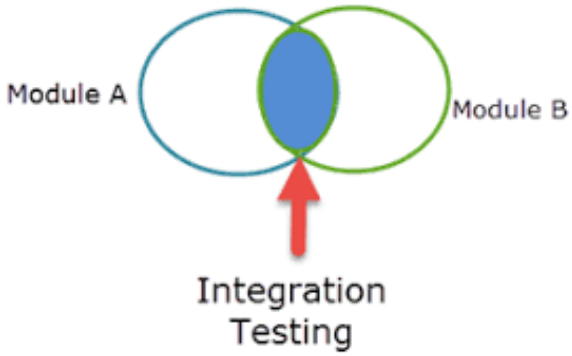


Figure 5.2: Integration Testing

program structure that has been overseen by the plot.

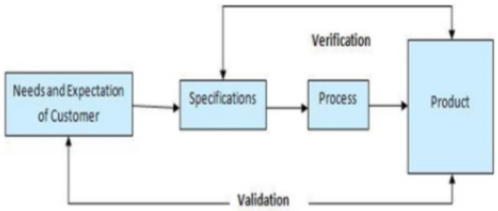


Figure 5.3: Validation Testing

5.1.3 Validation Testing

It starts toward the finish of coordination testing when specific parts have been worked out, the thing is totally gathered as a bundle, and interfacing bungles have been revealed and rectified (as appeared in Figure 5.2). At the endorsement or system level, the capability between ordinary programming, challenge orchestrated programming, and WebApps disappears. The way toward reviewing programming amidst the change framework or toward the fruition of the progressive strategy to pick if it fulfils chose business necessities. It guarantees that the thing genuinely addresses the customer's issues. It can in like way be portrayed as to exhibit that the thing fulls its typical use when sent on sensible condition. It addresses the inquiry, Are we making the correct thing?

5.1.4 Regression Testing

Each time new module is added prompts changes in program. This sort of testing ensure that entire segment works legitimately even subsequent to adding parts to the total program. Regression Testing is only a full or incomplete determination of effectively executed experiments which are re-executed to guarantee existing functionality work fine. Regression testing (once in a while non-relapse testing) is re-running useful and non-useful tests to guarantee that recently created and tried programming still performs after a change. If not, that would be known as a regression.

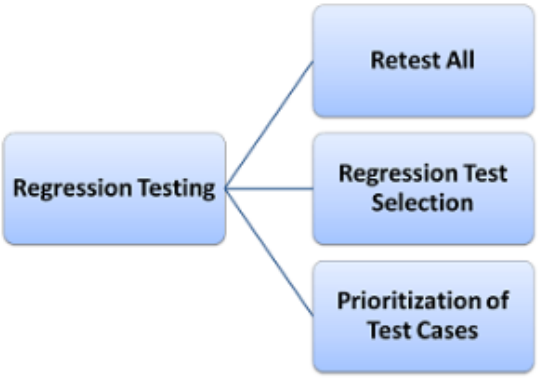


Figure 5.4: Regression Testing

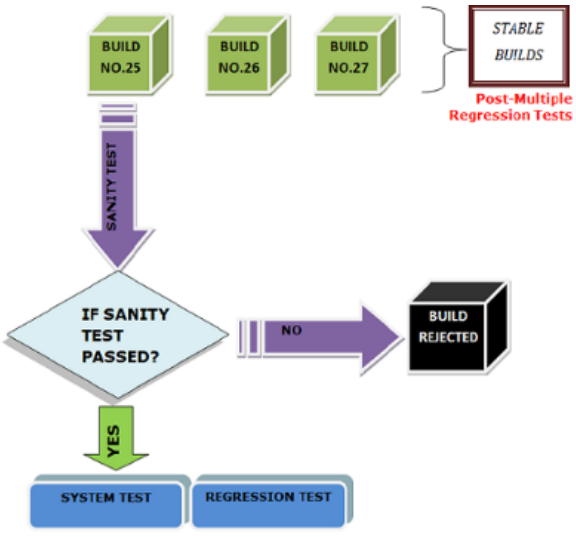


Figure 5.5: Regression Testing

5.1.5 Sanity Testing

Sanity testing is the subset of regression testing and it is performed when we don't possess enough energy for doing testing. Sanity testing is the surface dimension testing where QA engineer confirms that every one of the menus, capacities, directions accessible in the item and task are working fine.
Sanity testing, a product testing method performed by the test group for some essential tests. The point of the fundamental test is to be directed at whatever point another form is gotten for testing. Sanity test is typically unscripted, recognizes the ward missing functionalities. It is utilized to decide whether the segment of the application is as yet working after a minor change.
Sanity testing can be tight and profound. Sanity test is a restricted regression test that centers around one or a couple of regions of usefulness.

5.2 Test case details

5.2.1 Test case id: Creation of Genesis Block

Unit to test: Creation of Genesis Block
Assumptions: User has given correct credentials and user give atleast one value in during the transaction.
Test data: Variables and their values
Steps to be executed:
Expected result: It should create a block ID using the previous transaction ID and value of coins used.
Actual result: First block is created with a unique transaction ID using the passed values.
Pass/Fail: Pass
Comments: We have used BouncyCastle for the implementation of the SHA-256 for creation of the unique transaction ID.

5.2.2 Test case id: Making a transaction

Unit to test: Doing the transaction
Assumptions: Transaction is done by the valid user after getting authenticated and they are making transaction on valid products.
Test data: Number of value-coins available before and after the transaction and the transaction ID
Steps to be executed:
Expected result: Unspent transactions values remains consistent after the transaction. And the transaction ID generated is unique
Actual result: Wallet of the unspent transaction output remains consistent after the transaction and transaction ID is almost unique.
Pass/Fail: Pass
Comments: We have used the recipient private key, sender private key and number of coins passed

5.2.3 Test case id: Creating a barcode

Unit to test: Creation of Barcode
Assumptions: User is give all the correct values.
Test data: Values stored in the barcode and the product values.
Steps to be executed: Values are fed the zxing function to create the barcode
Expected result: Barcode should be created having all the values provided
Actual result: A barcode is created.
Pass/Fail: Pass
Comments: We have used Google's Zxing API for the creation of the barcode.

5.2.4 Test case id: Reading values from barcode

Unit to test: Reading of Barcode
Assumptions: User is reading the barcode correctly.
Test data: Values stored in the barcode and the product values.

Steps to be executed: Application is opened and add to cart is used to start the barcode scanner and scanning the barcode
Expected result: Barcode should be created having all the values provided
Actual result: A barcode is created.
Pass/Fail: Pass
Comments: We have used Google's Zxing API for the creation of the barcode.

5.2.5 Test case id: Adding coins into the wallet

Unit to test: Addition of coins in the application.
Assumptions: User is passing positive integer to the cart.
Test data: Value of the coins available in the wallet.
Steps to be executed: use of application functionality to add money and giving the value to be added.
Expected Result: Money is addded to the wallet correctly and a transaction ID is created which is unique for this user according to the timestamp and value of coins added.
Actual result: Everything went according to the expectation. Pass/Fail: Pass Comments: If user gives non negative integers, then only it will be forwarded to the next indent.

Chapter 6

Conclusions and Future Scope

The standard working of retail shops and their strategy for offering rewards rely upon the confidence and conviction that their clients have on them. So it is important to focus on the humongous favourable circumstances offered by the proposed innovation, and perform sufficient adjustments to execute it as the proposed framework guarantees wellbeing, honesty and potential advantages to the grocery store proprietors and to their clients. Their approach of offering faithfulness indicates and endeavours guarantee client maintenance and development of existing client system can be practised all the more monetarily and successfully utilizing the advanced stage is given by the blockchain innovation. Besides, the diminished exchange handling time and age of inexhaustibly accessible secure a piece of important organized information make it the most appropriate innovation to be joined with Big Data examination to forestall on the fly false exchanges and make a substantially more gainful business.

The epic plan introduced in this project is effective as to the present situation and could be conveyed in the genuine world.The normal working of retail shops and their technique for offering rewards rely upon the confidence and conviction that their clients have on them. So it is important to focus on the humongous points of interest offered by the proposed innovation, and perform satisfactory adjustments to execute it as the proposed framework guarantees security, trustworthiness and potential advantages to the general store proprietors and to their clients. Their procedure of offering dedication indicates and endeavours guarantee client maintenance and development of existing client system can be practised all the more financially

and viably utilizing the advanced stage is given by the blockchain innovation. Besides, the diminished exchange preparing time and age of liberally accessible secure and significant organized information make it the most reasonable innovation to be joined with Big Data investigation to counteract on the fly fake exchanges and make a substantially more beneficial business. The epic plan displayed in this paper is proficient with respect to the present situation and could be sent in reality.

With the usage of the proposed framework, the retailer would be free from utilizing individuals at the money counter. Rather, the retailer would now be able to utilize more individuals for various jobs like grocery store support and burglary counteractive action. Additionally by breaking down client item acquiring example a few on the fly customized plans and ads can be created to clear route for more noteworthy strategically pitching chances. New developing arrangements presented by new businesses like ShopKick can be utilized to increment in-store client traffic and addition better bits of knowledge into client buying designs whether in physical retail locations or on the web. Additionally, with the blend of Artificial Intelligence and Augmented Reality, it is conceivable to give the best client experience and administrations. At long last with the establishment of RFID labels and ink innovation for costly items and dress and sharp observing of the little measured things with the presentation of video examination it is conceivable to accomplish a robbery free condition at moderate speculation. Henceforth the proposed framework must be conveyed in reality to appreciate better benefits by the retailer and disentangle the client shopping background.

Bibliography

[1] Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, VÃŋctor SantamarÃŋa *To Blockchain or Not to Blockchain; That Is the Question* IEEE Computer Society On March/April 2018

[2] Ilya Sukhodolskiy, Sergey Zapechnikov *A Blockchain-Based Access Control System for Cloud Storage*. IEEE Computer Society On 2018 Issue No. : 978-1-5386-4340-2/18

[3] Leslie Mertz *(Block) Chain Reaction* IEEE Pulse Issue No. 2154-2287, 15 May 2018

[4] Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, *Blockchain and Smart Contract for Digital Certificate* IEEE International Conference on Applied System Innovation2018, Issue No. : 978-1-5386-4342-6

[5] Lael Brainard, *The Use Of Distributed Ledger Technologies in Payment, Clearing and Settlement* Board Of Governors Of The Federal Reserve System at Institute Of International Finance Blockchain Roundtable, Washington D.C. in April 14, 2016

[6] Harry Halpin and Marta Piekarska, *Introduction to Security and Privacy on the Blockchain* 2017 IEEE European Symposium on Security and Privacy Workshops (Euro S and PW)

[7] Ujan Mukhopadhyay, Anthony Skjellum, Oluwekemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks, *:A Brief Survey of Cryptocurrency Systems* IEEE

[8] Electrical and Computer Engineering (CCECE), *Bitcoin mining acceleration and performance quantification* 2014 IEEE 27th Canadian Conference on 4-7 May 2014, INSPEC Accession Number: 14599397

[9] O'guzhan Ersoy, Zhijie Ren, Zekeriya Erkin and Reginald L. Lagendijk, *Transaction Propagation on Permissionless Blockchains: Incentive and Routing Mechanisms* 2018 Crypto Valley Conference on Blockchain Technology

[10] Zhijie Ren, Kelong Cong, Taico V. Aerts, Bart. A.P. de Jonge, Alejandro F. Morais and Zekeriya Erkin, *A Scale-out Blockchain for Value Transfer with Spontaneous Sharding* 978-1-5386-7204-4/18 IEEE

[11] Sachchidanand Singh, Nirmala Singh *Blockchain: Future of Financial and Cyber Security* 2016 2nd International Conference on Contemporary Computing and Informatics (ic3i)

[12] Arpita Nayak, Kaustubh Dutta *Blockchain: The Perfect Data Protection Tool* 2017 International Conference on Intelligent Computing and Control (I2C2)

[13] Miguel Villarreal-Vasque, Denis Ulybyshe, Bharat Bhargava, Ganapathy Mani, Jason Kobes Northrop Grumman, Paul Conoval, Robert Pike, Steve Seaberg *âĂŸBlockhubâĂŹ: Blockchain-based Software Development System for Untrusted Environments* 2018 IEEE 11th International Conference on Cloud Computing, 2159-6190/18

[14] Li Shuling *Application of Blockchain Technology in Smart City Infrastructure* 2018 IEEE International Conference on Smart Internet of Things, 978-1-5386-8543-3

[15] Konstantinos Christidis, Michael Devetsikiotis, K. Christidis *Blockchains and Smart Contracts for the Internet of Things*

[16] Tien Tuan Anh Dinh , Rui Liu, Meihui Zhang , Gang Chen, Beng Chin Ooi, and Ji Wang *Untangling Blockchain: A Data Processing View of Blockchain Systems*

[17] Chris SkinnerâĂŹs Blog: *https://thefinanser.com/* [accessed on 17th Jan 2019]

[18] L.M. Bach, B. Mihaljevic and M. Zagar *Comparative analysis of Blockchain Consensus Algorithms* MIPRO 2018, May 21-25, Opatija Croatia, 1545-1551

[19] John R. Douceur *The Sybil Attack* International Workshop on Peer-to-Peer Systems, IPTPS 2002: Peer-to-Peer Systems pp 251-260

[20] Bozhi Wang, Shiping Chen, Lina Yao , Bin Liu, Xiwei Xu and Liming Zhu *A Simulation Approach for Studying Behavior and Quality of Blockchain Networks* Springer International Publishing AG, part of Springer Nature 2018 S. Chen et al. (Eds.): ICBC 2018, LNCS 10974, pp. 18âĂŞ31, 2018

[21] Speturn IEEE: *https://spectrum.ieee.org/computing/networks/how-blockchains-work* [accessed on 18th Jan 2019]

[22] Hackernoon: *https://hackernoon.com/the-difference-between-traditional-and-delegated-proof-of-stake-36a3e3f25f7d* [accessed on 20th Jan 2019]

[23] Thomas Burke *The Essential Diversity of Blockchain Nodes* CACI, International IEEE Blockchain Newsletter, December 2018

[24] Stefano De Angelis , Leonardo Aniello , Roberto Baldoni, Federico Lombardi, Andrea Margheri , and Vladimiro Sassone, *PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain* Research Center of Cyber Intelligence and Information Security, Sapienza University of Rome

[25] Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang *Blockchain challenges and opportunities* Int. J. Web and Grid Services, Vol. 14, No. 4, 2018, 352-376

[26] Clique Algorithm: GitHub *https://github.com/ethereum/EIPs/issues/225* [accessed on 25th Feb 2019]

[27] Go-Ethereum: *https://geth.ethereum.org* [accessed on 25th Feb 2019]

[28] G. Wood *Ethereum: A secure decentralised generalised transaction ledger.* Ethereum Project Yellow Paper, 2014

[29] Wiley series *Pattern-oriented software architecture: A system of Patterns, volume 1*

[30] Gautier Marin's Blog: *https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d* [accessed on 28th Feb 2019]

[31] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System: www.bitcoin.org* [accessed on 01st March 2019]

[32] ShawnTabrizi *A Next-Generation Smart Contract and Decentralized Application Platform* https://github.com/ethereum/wiki/wiki/White-Paper [accessed on 2nd March 2019.