SOLUTION TO COUPON FRAUD PROBLEM USING BLOCKCHAIN

A PROJECT REPORT

submitted by

ASHWIN MADHU (TVE17MCA012)
VARNA KRISHNAN P E (TVE17MCA052)
VYSHAK PUTHUSSERI (TVE17MCA054)

to

the APJ Abdul Kalam Technological University
in partial fullfilment of the requirements for the award of the degree

of

Master of Computer Applications

Department of Computer Applications
College of Engineering Trivandrum
Trivandrum-695016

NOVEMBER 2019

DECLARATION

We undersigned hereby declare that the project report SOLUTION TO CUSTOMER LOYALTY PROBLEM, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Prof. Baby Syla. This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. We also declare that We have adhered to ethics of academic honesty and integrity as directed in the guidelines of Institutional ethics committee of the college and have not misrepresented or fabricated any data or idea or fact or source in my submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title.

Place : Trivandrum
Date : 20-11-2019

Ashwin Madhu
Varna Krishnan P E
Vyshak Puthusseri

DEPARTMENT OF COMPUTER APPLICATIONS

COLLEGE OF ENGINEERING TRIVANDRUM

CERTIFICATE

This is to certify that the report entitled **SOLUTION TO COUPON FRAUD PROBLEM USING BLOCKCHAIN** submitted by **Ashwin Madhu** & **Varna Krishnan P E** & **Vyshak Puthusseri** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications is a bonafide record of the project work carried out by her under my guidance and supervision. This report in any form has not been submitted to any University or Institute for any purpose.

Head of the Dept

Project Guide

ACKNOWLEDGEMENT

If words are considered as symbols of approval and tokens of acknowledgement, then let words play the heralding role of expressing my gratitude.

First of all, I would like to thank God almighty for bestowing me with wisdom,courage and perseverance which had helped me to complete this project ***SOLUTION TO COUPON FRAUD PROBLEM USING BLOCKCHAIN***. This project has been a reality as a result of the help given by a large number of personalities.

I am extremely thankful to **Dr Jiji C V**, Principal, College of Engineering Trivandrum for providing me with the best facilities and atmosphere which was necessary for the successful completion of this project.

I would like to remember with gratitude **Dr. Sabitha S**, Head Of Department Department of Computer Applications, College of Engineering, Trivandrum for the encouragement and guidance rendered.

I express my sincere thanks to **Prof. Baby Syla L**,Associate Professor, Department of Computer Applications, College of Engineering Trivandrum for her valuable guidance, support and advice that aided in the successful completion of my project.

Finally, I wish to express my sincere gratitude to all my friends, who directly or indirectly contributed in this venture.

Ashwin Madhu
Varna Krishnan P E
Vyshak Puthusseri

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The paper coupon market has been with us almost since shopping was first invented. Practically all retail outlets, big or small, have used coupons at least once in their lives. The primary motivation is either to attract more customers by offering them a discount or to enable them to pay in advance for gift vouchers that are subsequently passed on to third parties. The major disadvantage of the paper based coupon was its cost and difficulties in distribution of the coupons. Also the accounting process becomes extremely time consuming. There are issues related to study the market feedback. A very high proportion of paper coupons are never returned. Paradoxically, a bigger problem is that no firm evidence can be identified to help explain why some actually are returned! All these problems can be solved by digitizing the coupon industry. But a major problem arises due to the arrival of digital coupons. The coupons are getting manipulated by some individuals, which causes a lot of loss to the merchants. So in many situations the loyalty of the customer has to be cross validated by the retailers.

With the normal encryption mechanism, up to a certain extent this problem can be solved. But if the attacker was highly skilled with tremendous computation power those techniques wont last long. We approach this problem with the disruptive technology, the blockchain. The retailers can generate coupons for a particular product and can share it with the universe using any social media. The coupons are stored in an open source blockchain platform called Ethereum. With the underlying security mechanism of the ethereum blockchain, our system was tamper-proof, as till date nobody was able to break the blockchain network.

Blockchain is a distributed ledger that was originally proposed as the underlying technology for bitcoin and other cryptocurrencies, and has since been applied to non-monetary applications. Blockchain is immutable as it is jointly managed by network participants through a consensus mechanism, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or Proof-of-ElapsedTime (PoET). Consensus delivers agreement among the network participants, which are untrusted, on the current state of the ledger. In effect, trust in the current state is decentralised due to its coupling to the outcome of distributed consensus among the participants.

2.3.2 Software Requirements

- Linux
- Ethereum blockchain
- NodeJS
- Web3 framework

2.4 Functional Requirements

Functional requirements outline the intended behaviour of the system. This behaviour may be denoted as tasks or functions that the specified system is intended to perform.

2.4.1 Web Interface

A web interface facilitates the interaction of the users with the system. The manufacture adds the retailer, retailer generates the discount coupon. A QR code is used corresponding to each coupon, this QR code get scanned and discount get redeemed by the customers.

2.4.2 NodeJs

Node.js is an open source, cross-platform runtime environment for developing server-side and networking applications. Node.js applications are written in JavaScript, and can be run within the Node.js runtime on OS X, Microsoft Windows, and Linux.Node.js also provides a rich library of various JavaScript modules which simplifies the development of web applications using Node.js to a great extent.

2.4.3 Web3.js

web3.js is a collection of libraries which allow you to interact with a local or remote ethereum node, using a HTTP or IPC connection. Web3.js enables you to develop websites or clients that interact with the blockchain - writing code that reads and writes data from the blockchain with smart contracts. It works by developing clients that interact with The Etherem Blockchain. It is a collection of libraries that allow you to perform actions like send Ether from one account to another, read and write data from smart contracts, create smart contracts, and so much more

2.4.4 Ethereum Blockchain

Ethereum blockchain is very much similar to the bitcoin network. Ethereum blockchain provides a platform to build decentralized applications known as Dapps. Similar to the bitcoin network, Ethereum is purely decentralised. One of the factors that distinguish Ethereum blockchain from bitcoin is that it is programmable. In addition to the transactions, each block in the blockchain contains a code snippet called smart contracts. It helps in bringing together people and organisations from different dimensions of society without any third party dependency. Ethereum blockchain contains blocks of transactions. Each block contains a list of transactions and a code snippet called smart contract. Ethereum uses an algorithm called proof of work algorithm to verify the entire network. An important data structure that is used by Ethereum is the Merkle tree. Each and every transaction in Ethereum is represented by a hash value. Merkle tree is a tree made of transaction hash values. Inside a block, two transactions are paired to form a single hash. Then two paired transactions together form another hash. This process continues until we get a single hash at the root. The root of a Merkle tree will be an outcome of the entire transactions within that block.

2.4.4.1 Smart Contract

Smart contracts are the crucial components which live inside the blocks of blockchain in the form of snippets of code. Solidity is the most popularly used smart contract programming language. The solidity code is very similar to javascript. Smart contracts are a set of rules and conditions which has to be followed during transactions. Smart contracts are an integral part as it eliminates the need for trusted third parties.

2.4.4.2 Ganache

In order to simulate blockchain Ganache is used. Ganache is a personal blockchain for Ethereum development you can use to deploy contracts, develop your applications, and run tests. It is available as both a desktop application as well as a command-line tool (formerly known as the TestRPC). It gives you the ability to perform all actions you would on the main chain without the cost. Many developers use this to test their smart contracts during development. It provides convenient tools such as advanced mining controls and a built-in block explorer.

2.4.4.3 Truffle

Truffle is a developer environment, testing framework and asset pipeline for blockchains. It allows developers to spin up a smart contract project at the click of a button and provides you with a project structure, files, and directories that make deployment and testing much easier.A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier. With Truffle, you get:

- Built-in smart contract compile, deploy, link and binary management.
- Scriptable, extensible deployment migrations framework.
- Network management for deploying to any number of public private networks.
- Package management with EthPM NPM, using the ERC190 standard.
- Interactive console for direct contract communication.

2.5 Non Functional Requirements

Non-Functional requirements define the general qualities of the software product. Non-functional requirement is in effect a constraint placed on the system or the development process. They are usually associated with product descriptions such as maintainability, usability, portability, etc. it mainly limits the solutions for the problem. The solution should be good enough to meet the non-functional requirements.

2.6 Quality Requirements

- Transparency: Transparency in blockchain defines the ability to access transaction history, assets etc. without limitations or boundaries. The system is transparent as anyone who is taking part in the system can verify the coupons generated.
- Reliability: Blockchain is considered reliable because full copies of the blockchain ledger are maintained by all active nodes. Thus, if one node goes offline, the ledger is still readily available to all other participants in the network. A blockchain lacks a single point of failure.
- Consistency: Consistency guarantee that all honest parties output the same sequence of blocks throughout the execution of the protocol.

Chapter 3

Design And Implementation

3.1 Design

3.1.1 Overall Design

Our system is a blockchain based digital coupon validation system. The system enables the retail chains to issue coupons. The retailers can verify the coupon when the customer came to redeem it. It also makes the verification much more efficient by enabling customers and retailers to verify the genuineness of the coupons. And there by enabling the solution to the customer loyalty issues.

3.1.2 User Interfaces

One of the main aims while designing the system was to abstract as much lower level details of the system as possible from the user. This system provides a web interface for its users. The interface is developed using NodeJS's Express framework.

3.1.3 System Design

The only technology on earth today that could handle all these problems and provide us with immutable, verifiable and trustworthy certificates is 'Blockchain'. The proposed system uses the public blockchain technology called Ethereum blockchain and the highly distributed. Here the focus is on solving the problem with the digital coupons storing and validation. This system provides the retailers to verify the genuinely of the coupons brought by the customer.

3.2 Implementation

3.2.1 Creating the discount coupon

The authenticated retailer can add discount to a particular product with a particular time validity. Those data was hashed using the sha256 algorithm and was stored in an etherum blockchain. The hashed code will be published and will be shared in various media in the form of a QR code for better representation.

Whenever the retailer added a new discount coupon, he can create the respective coupons and will publish it.

3.2.2 Verifying the coupon

The customer can bring those coupons and redeem them for a particular product. A coupon will only work for that particular product. All those constraint checking was done at the time of verifying. From the scanned QR code, the hash code will be detected, and it will be matched with the particular index of the deployed contract. By using the corresponding index, the aggregate data can be retrieved.

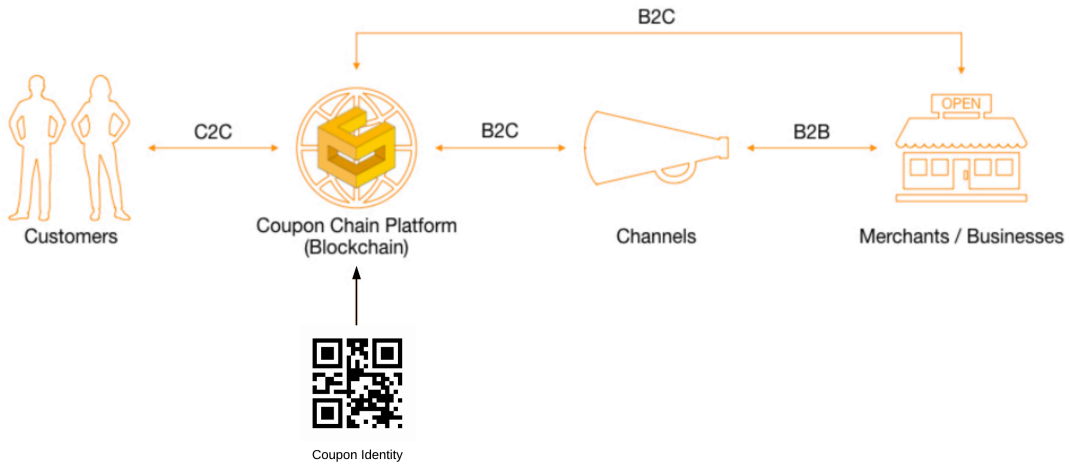


Figure 3.1: System Design

3.3 Data Flow Diagrams for the System

These diagrams gives a clear picture about the privileges of each user. Also the entire working flow was specified in this. The DFDs are as follows:

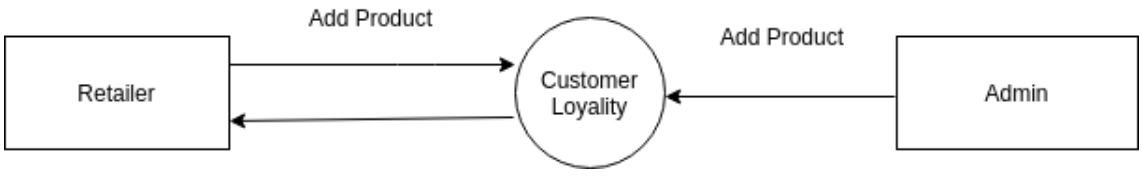


Figure 3.2: Level 0.1 Data Flow

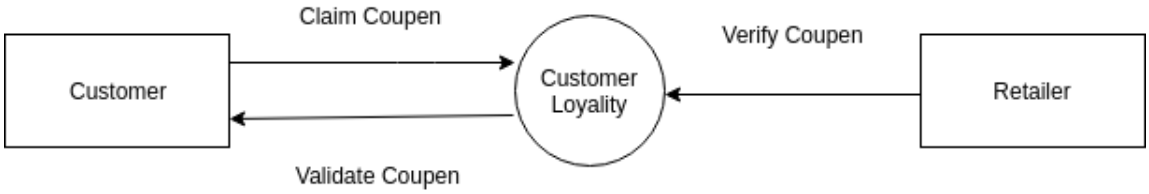


Figure 3.3: Level 0.2 Data Flow

There are three users in this project mainly admin, retailers and customers. In DFD level 0.1 retailers and admins take part. The user admin communicates with the system by adding products and retailers. Also retailers can add products at this level. In DFD level 0.2 customers and retailers take their role. Customers can claim and validate the coupons and retailers can verify the coupons.

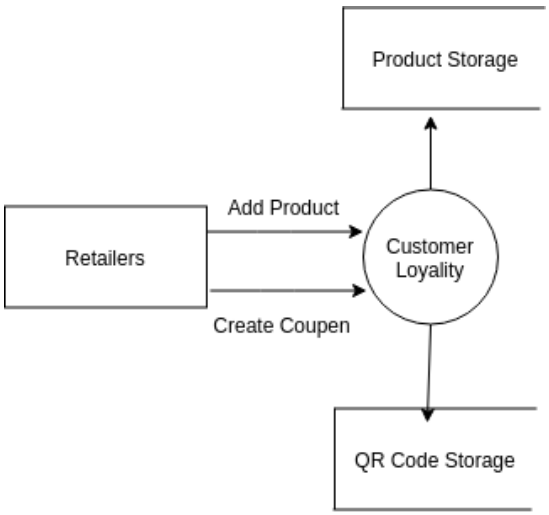


Figure 3.4: Level 1.1 Data Flow

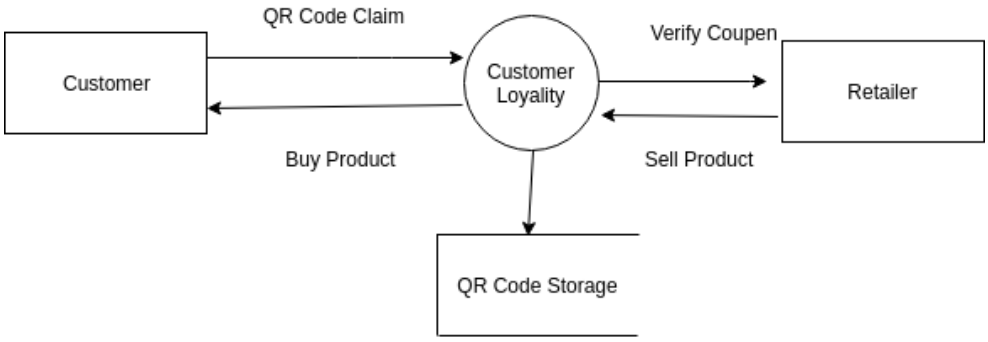
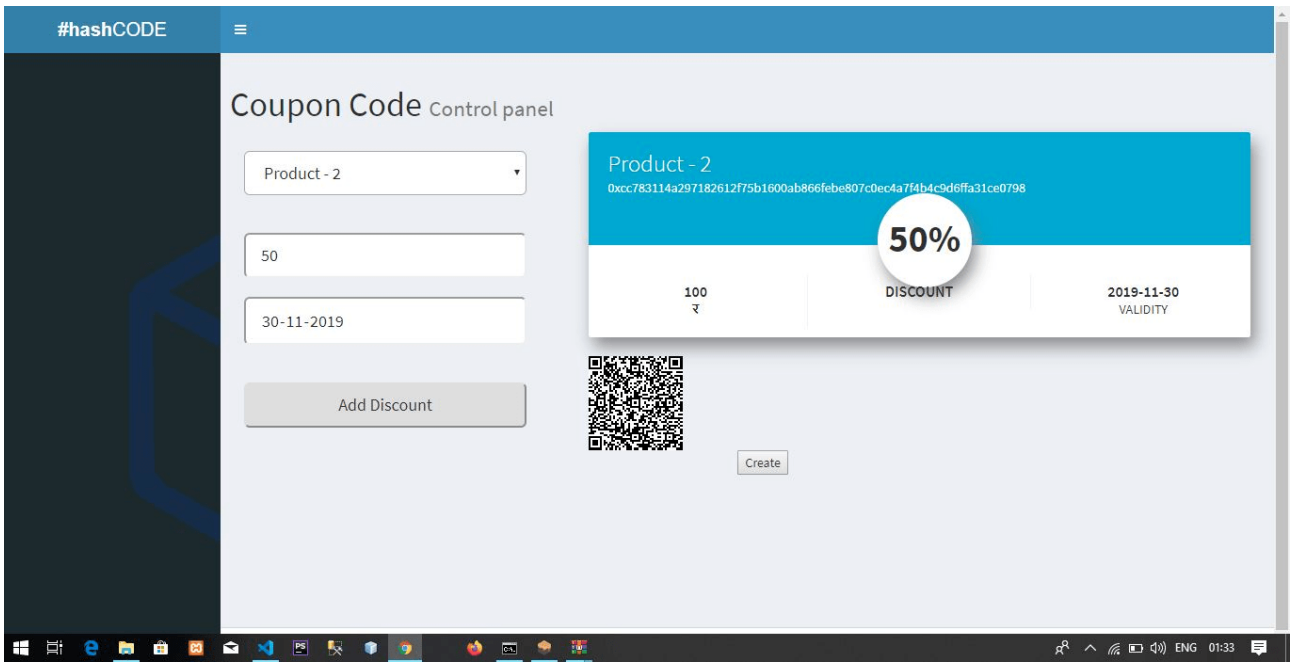
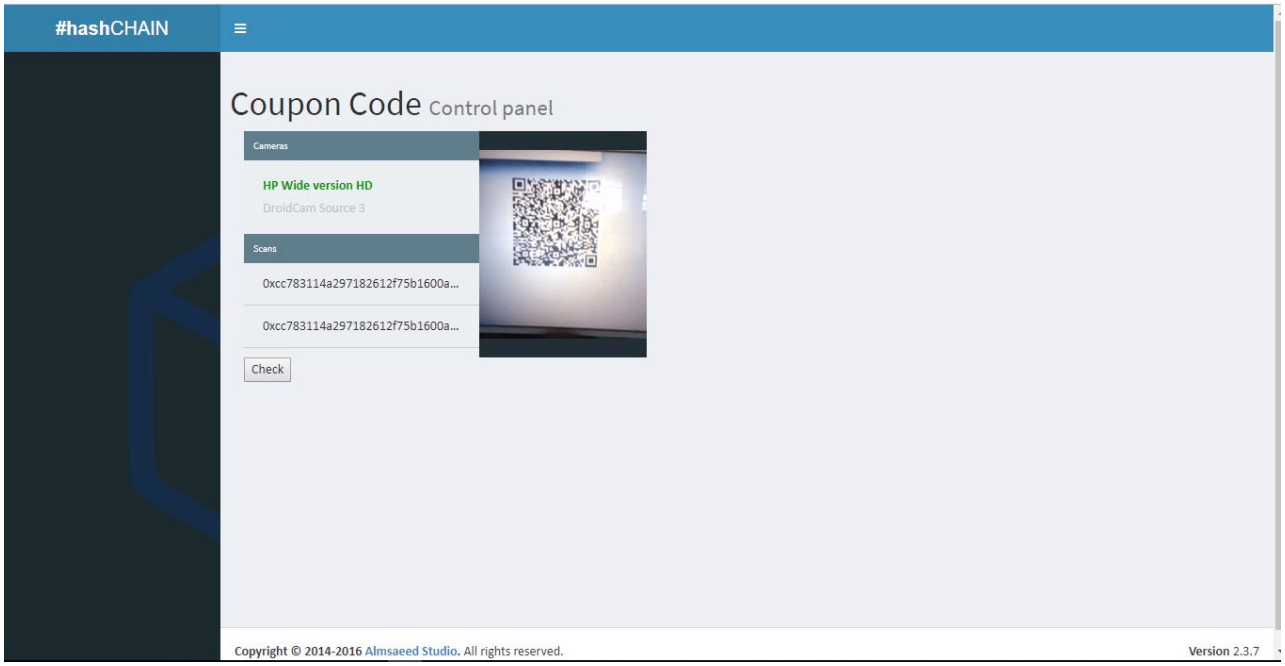


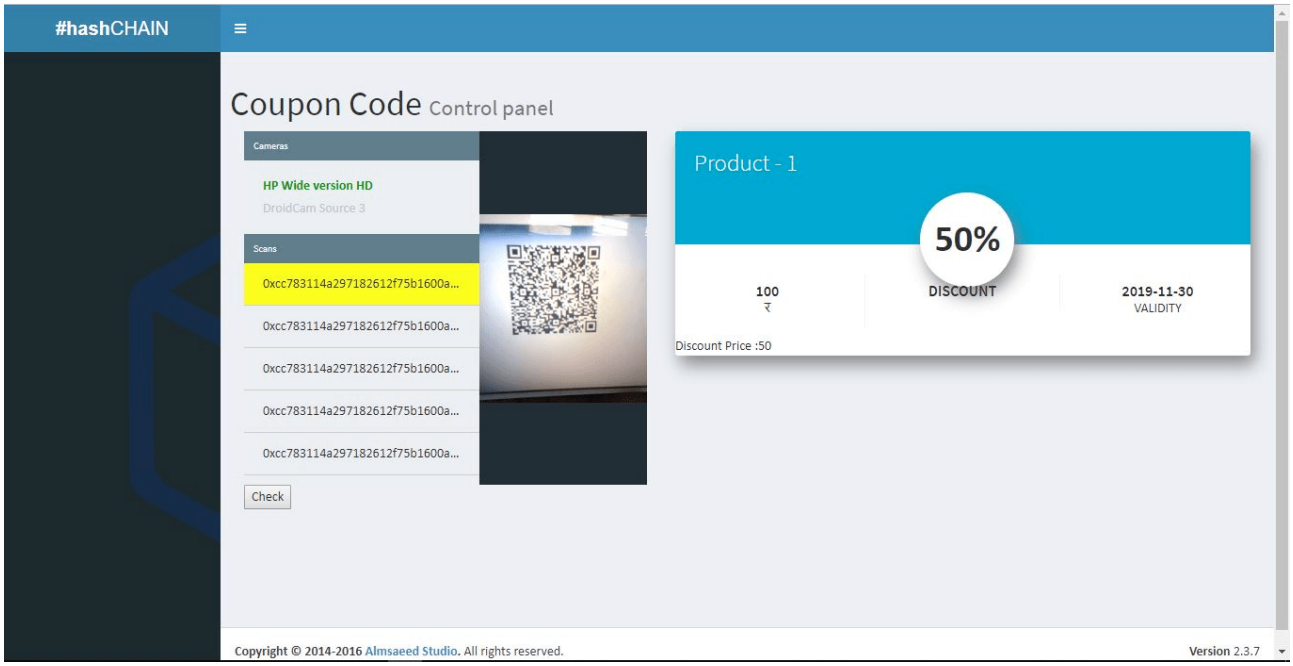
Figure 3.5: Level 1.2 Data Flow

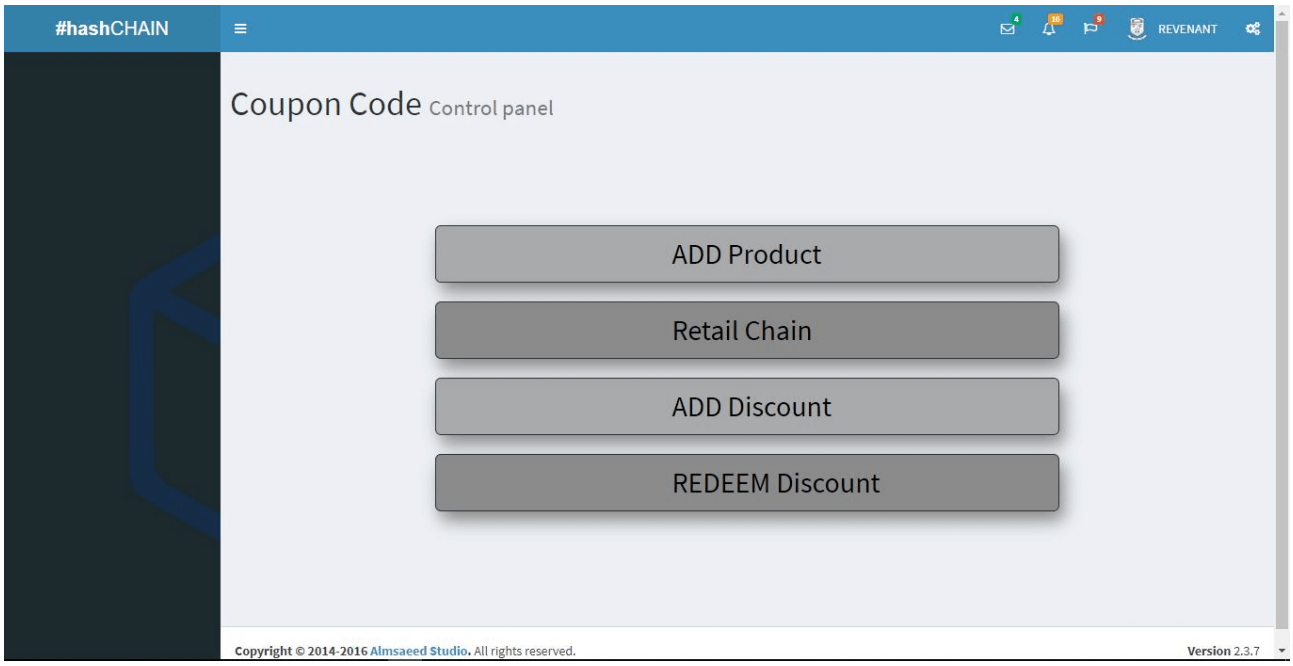
Levels 1.1 and 1.2 gives the detailed operation of the previous DFD. The product added by the retailer is stored in the blockchain storage. The retailers can generate the discount coupon and corresponding hash value will be stored and published as a QR code. In level 1.2 the customer can claim the coupon and buy the product and the retailer can verify the product and sell the product.

3.3.1 Screenshots






#hashCHAIN
Coupon Code Control panel
Cameras
HP Wide version HD
DroidCam Source 3
Scans
0xcc783114a297182612f75b1600a...
0xcc783114a297182612f75b1600a...
0xcc783114a297182612f75b1600a...
0xcc783114a297182612f75b1600a...
0xcc783114a297182612f75b1600a...
Check
Product - 1
50%
100
₹
DISCOUNT
2019-11-30
VALIDITY
Discount Price :50
Copyright © 2014-2016 Almsaeed Studio. All rights reserved.
Version 2.3.7


#hashCHAIN
REVENANT
Coupon Code Control panel
ADD Product
Retail Chain
ADD Discount
REDEEM Discount
Copyright © 2014-2016 Almsaeed Studio. All rights reserved.
Version 2.3.7

Chapter 7

Conclusion

The retailers create a promo code for a particular product with some discount and add the corresponding details get added into the blockchain. Corresponding to the data added, a hash value gets generated. Using the hash value, a QR code is going to be generated, and which is going to be publicly advertise. The customer with that QR code can go to a verified dealer and he can give the discount as prescribed. Till date no one was able to tamper the blockchain technology and so our system. The system provides permanent solution for the customer locality problem, makes it easily accessible from anywhere and everywhere. Cryptography protection ensures that the data is tamper-proof and immutable. The digital coupons help us to avoid the delay in physically doing the transactions. Moreover, it can help us to save time. It solves all such problems of traditional coupon industry. The implementation of this system will mop off fake coupons generation and manipulations.

DEPARTMENT OF COMPUTER APPLICATIONS

COLLEGE OF ENGINEERING TRIVANDRUM

CERTIFICATE

Certified that this Seminar report entitled, ***"A Style-Based Generator Architecture for Generative Adversarial Networks"*** *is the paper presented by* ***" VYSHAK PUTHUSSERI" (Reg No: TVE17MCA054)*** *in partial fulfillment of the requirements for the award of the degree of Master of Computer Applications of APJ Abdul Kalam Technological University during the year 2019.*

Prof. Jose T Joseph. Dr. Sabitha. S

Co-ordinator **Head of the Department**

Acknowledgement

First and for most I thank **GOD** almighty and to my parents for the success of this seminar. I owe a sincere gratitude and heart full thanks to everyone who shared their precious time and knowledge for the successful completion of my seminar.

I would like to thank **Dr Jiji C V**, Principal, College of Engineering Trivandrum, who helped me during the entire process of work.

I am extremely grateful to **Dr.Sabitha S**, HOD, Dept of Computer Applications, for providing me with best facilities and atmosphere for the creative work guidance and encouragement.

I would like to thank my coordinator, **Prof.Jose T Joseph**, Dept of Computer Applications, who motivated me throughout the work of my seminar.

I profusely thank other Asst. Professors in the department and all other staffs of CET, for their guidance and inspirations throughout my course of study.

I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this seminar. No words can express my humble gratitude to my beloved parents and relatives who have been guiding me in all walks of my journey.

Vyshak Puthusseri

Chapter 1

Introduction

Deep learning is an artificial intelligence function that imitates the workings of the human brain in processing data and creating patterns for use in decision making. Deep learning is a subset of machine learning in artificial intelligence (AI) that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Also known as deep neural learning or deep neural network. Deep Learning is about learning multiple levels of representation and abstraction that help to make sense of data such as images, sound, and text.

In Artificial Intelligence (AI), we can think of machine learning (ML) as one of AI's smaller subsets. Machine learning uses statistical techniques to provide computer systems ability to progressively improve its performance on a specific task with data without being explicitly programmed. Unsupervised learning algorithms are a subset of machine learning algorithms which tries to describe the structure of unlabelled data. Generative models is an approach to unsupervised learning. The goal of a generative model is to generate data similar to the ones in the dataset. Generative Adversarial Network (GAN) is a type of Generative Model. Other types of generative models include Variational Autoencoders (VAEs) and autoregressive models like PixelRNN. GANs have been successfully applied to solve problems in various domains like generating images, videos and audio, text to image synthesis etc. GANs were originally introduced by Ian Goodfellow and his collaborators in University of Montreal in 2014 . Yann LeCun, Director of AI Research at Facebook and Professor at NYU called adversarial training as "the most interesting idea in the last 10 years in ML" .

Deep learning is a subset of machine learning in artificial intelligence (AI) that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Also known as deep neural learning or deep neural network. The resolution and quality of images produced by generative methods especially generative adversarial networks (GAN) have seen rapid improvement recently. Yet the generators continue to operate as black boxes, and despite recent efforts, the understanding of various aspects of the image synthesis process, e.g., the origin of stochastic features, is still lacking.

Pooling layers section would reduce the number of parameters when the images are too large. Spatial pooling also called subsampling or downsampling which reduces the dimensionality of each map but retains the important information. Spatial pooling can be of different types:

- Max Pooling
- Average Pooling
- Min pooling

Flattened the feature map into a one dimensional vector and feed it into a fully connected layer of a Deep neural network.

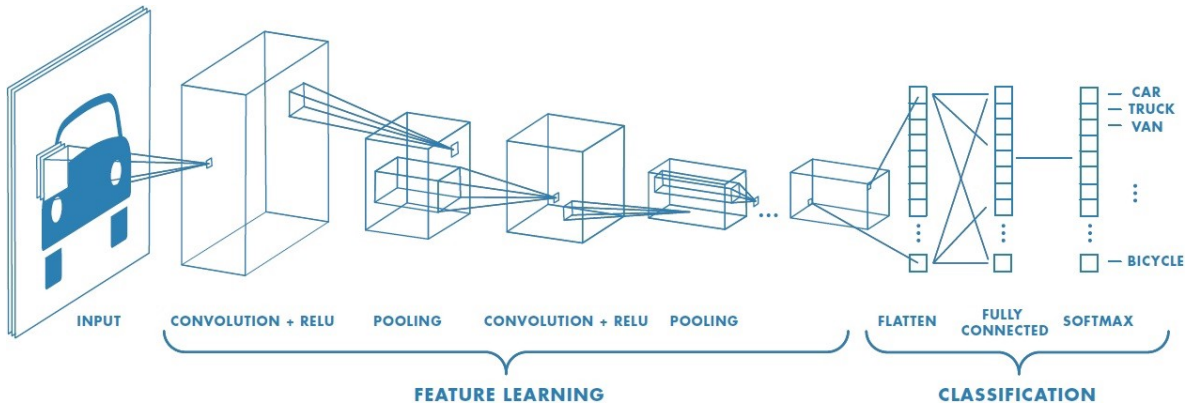


Figure 1.5: Convolutional Neural Network model

of correlated features) for the tensors output by the style-layers. The Gram-matrix is essentially just a matrix of dot-products for the vectors of the feature activations of a style-layer. If an entry in the Gram-matrix has a value close to zero then it means the two features in the given layer do not activate simultaneously for the given style-image. And vice versa, if an entry in the Gram-matrix has a large value, then it means the two features do activate simultaneously for the given style-image. We will then try and create a mixed-image that replicates this activation pattern of the style-image.If the feature map is a matrix F, then each entry in the Gram matrix G can be given by:

$$Gij = \sum_{k} FikFjk$$

The loss function for style is quite similar to out content loss, except that we calculate the Mean Squared Error for the Gram-matrices instead of the raw tensor-outputs from the layers.

$$Lstyle = \frac{1}{2}\left(\sum_{i=0}^{L}(Gij - Aij)^2\right)$$

As with the content representation, if we had two images whose feature maps at a given layer produced the same Gram matrix we would expect both images to have the same style, but not necessarily the same content. Applying this to early layers in the network would capture some of the finer textures contained within the image whereas applying this to deeper layers would capture more higher-level elements of the image's style. Gatys et. al [1] found that the best results were achieved by taking a combination of shallow and deep layers as the style representation for an image. The best results are achieved by a combination of many different layers from the network, which capture both the finer textures and the larger elements of the original image.

2.3 Optimizing loss function and styling the image

Using a pre-trained neural network such as VGG-16, an input image (i.e. an image which provides the content), a style image (a painting with strong style elements) and a random image (output image), one could minimize the losses in the network such that the style loss (loss between the output image style and style of 'style image'), content loss (loss between the content image and the output image) and the total variation loss (which ensured pixel wise smoothness) were at a minimum. In such cases, the output image generated from such a network, resembled the input