Using cryptocurrency along with smart contracts to create a social platform

A dissertation submitted for
the Degree of Master of Computer Science

G. KULASANGAR
University of Colombo School of Computing

2019

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name: G.Kulasangar

Registration Number: 2016/mcs/033

Index Number: 16440335

_____

Signature: Date:

This is to certify that this thesis is based on the work of

Mr./Ms.

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

_____

Signature: Date:

Acknowledgements

This thesis is the result of me being fortunate to have the unconditional assistance of several people who have been extremely supportive in various ways. First and foremost, I would like to offer my humble gratitude to Dr. Kasun de Zoysa, my supervisor, for their tremendous encouragement, support and the guidance given throughout this research.

I would like to sincerely thank all the lecturers at the University of Colombo School Of Computing for their valuable advices and comments given at various stages of this research. Without your support, I could not have completed this research with success.

I like to thank all my dear friends who were there around me, with best of their encouragement, suggestions and support throughout this research.

Finally, I would like to express my heartfelt thanks towards my family for their support and encouragement through the many days and nights dedicated to the completion of this research.

Abstract

The common problem in this era, is that the companies or websites which are being utilized by the consumers, or rather the public, have been providing services solely for their own business growths and profits. Which ideally, leaves the customers to limited resources, based on the amount they pay. The community related apps or websites these days, aren't about contributing and benefitting from or to the community. It's about entirely receiving the benefits. Hence the motivation towards this research component is that, to create a platform which is entirely decentralized, and any benefits and contributions will be made by the users themselves. The benefits to the customer base would be given in the form of a digital currency.

Existing applications which are out there in the world, are pretty much storing the user's personal data, and holding the ownership of those data. These data are being stored in servers which are spread across the globe, which could be either owned by Google or Apple or Microsoft. The concept of SMART Contract will be utilized as the middleman between all the consumers or users and the application, in order to make sure that the appropriate user is given the relevant privileges to gain or contribute from or to the community. So that the consensus problem is being rectified and makes sure that there won't be any frauds or manipulations within the community.

Having a decentralized application would make sure that the users of the application are aware that their personal information can only be altered by themselves, not by anyone else. So as a proof of study, in order to prove that applications can be built as decentralized so that only the users will be benefited with the services. Along with the increase of population here in Sri Lanka, most of the people do travel by using the public transport, ie. Train, Bus. As an example, most of the people are still struggling to figure out the daily schedule (departure and arrival) and the time duration for a whole journey of a train, which would ideally make every single public's daily plans even worse. Since the people are quite unsure of the time, when the train would leave or arrive from or to a station, they will have to be at the station way early than normal in order to make sure that they catch the train or either they might get late to reach a destination. Hence, it's easy for people, if they're aware well ahead of this, they can decide accordingly.

In order to do that, I'm trying to build up a community platform where the users are the public (contributors + non-contributors), and they can contribute to the community in order to earn themselves some benefits from the application. So the platform would be using the Ethereum's Ether, which is a cryptocurrency just like Bitcoin, as the benefit for the user and the core of this platform would be utilizing the concept of Smart Contract which relies on the abstraction of Blockchain which is a decentralized chain which keeps the track of the relevant information of all the users and their relative tokens within the network.

List of Tables

List of Figures

List of Acronyms

D-App	Decentralized Application
R&D	Research and development
LOD	Level Oriented Design
EVM	Ethereum Virtual Machine
IDE	Integrated Development Environment

TABLE OF CONTENTS

Chapter 1 – Introduction

1.1 Overview

This chapter provides a brief description of using crypto currency for social related decentralized applications and importance of the study. This study elaborates about why crypto currency is important in doing transactions or why we need smart contracts on the longer run, without any middle man to take all the decisions. Furthermore, the chapter describes the background of the study, its aims and objectives and the significance in the following sections respectively.

1.2 Background of the study

The common problem in this era, is that the companies or websites which are being utilized by the consumers, or rather the public, have been providing services solely for their own business growths and profits. Which ideally, leaves the customers to limited resources, based on the amount they pay. The community related apps or websites these days, aren't about contributing and benefitting from or to the community. It's about entirely receiving the benefits. Hence the motivation towards this research component is that, to create a platform which is entirely decentralized, and any benefits and contributions will be made in the form of a digital currency by the users themselves.

The thesis reports the findings of a thorough study, to establish the factors that have led to the success of decentralized applications, which are written based on smart contracts and how such factors can be applied in developing any kind of community-based application. It can also be contended that, the awareness of the users who are using the existing web or mobile applications which are related to any kind of services, they just provide their confidential information to the application providers, pay for the services and utilize them. But then, there's no such functionality or rather a feature where the user can give something back to the community and make the privileges and information more of decentralized, so that they don't reveal their personal information, which could be critical when an anonymous organization tries to retrieve that information.

However, based on the findings, there have been few web applications such as steemit, which is basically a community-based service, where it's purely decentralized and the incentives for the users are being given as digital currencies. Even though an application is considered as decentralized, numerous factors should be taken into consider before transferring the digital currencies in between the end users. The possible threats could be the security of the application, handling the wallets and identifying any spam users. In order to rectify those issues, there are secure mechanisms which can be adopted in order to do those, payment transactions.

1.3 Aims and Objectives

The core objectives of this project are that, giving a consistent platform for the users to contribute and gain benefits based on their contribution in order to identify where a current train is, and how long has it taken to reach there, and what station would it reach next, which trains are available in a given period etc.

The users will be given tokens as credits for every contribution they've made, and they can use it in order to utilize the functions and features of the application. The tokens would vary depending on the level of the contribution of the user. So simply in order to earn tokens, the user will have to contribute to the community platform, if not he/she will not be able to utilize all the features of the application.

1.4 Scope of the project

The reason behind having boundaries within a project is that, to reduce the complexity of the project and to narrow down the project research area within a circle so that the requirements to be done and the proof of work is clear. Some of the boundaries which I'm trying to create is that, this community platform is totally for the users who are travelling by trains daily or occasionally. This platform could be applied to many business scenarios which would ideally make the scope look a bit complex.

There are few assumptions which had to be taken along the project which should be gradually removed, and more comprehensive and broad decisions should be made.
Hence the assumptions are:

- The wallet to store the tokens should be created by the user themselves
- As from the application perspective, key decisions should be made to read and write transactions securely from the wallet. The mechanism to prevail the reliability and the certainty of the transactions.
- Based on what scenarios the tokens are going to be awarded.
- If there are ads on the application, how the value would impact on all the users

1.5 Motivation

So as a proof of study, in order to prove that applications can be built as decentralized so that only the users will be benefited with the services. Along with the increase of population here in Sri Lanka, most of the people do travel by using the public transport, ie. Train, Bus. As an example, most of the people are still struggling to figure out the daily schedule (departure and arrival) and the time duration for a whole journey of a train, which would ideally make every single public's daily plans even worse. Since the people are quite unsure of the time, when the train would leave or arrive from or to a station, they will have to be at the station way early than normal in order to make sure that they catch the train or either they might get late to reach a destination. Hence, it's easy for people, if they're aware well ahead of this, they can decide accordingly.

In order to do that, the author's trying to build up a community platform where the users are the public (contributors + non-contributors), and they can contribute to the community in order to earn themselves some benefits from the application. So the platform would be using the Ethereum's Ether, which is a cryptocurrency just like Bitcoin, as the benefit for the user and the core of this platform would be utilizing the concept of Smart Contract which relies on the abstraction of Blockchain which is a decentralized chain which keeps the track of the relevant information of all the users and their relative tokens within the network.

1.6 Thesis Outline

The thesis is organized as follows:

Chapter 2, Literature Review describes the current researches about the existing decentralized applications and the way they have used crypto currency, blockchain and smart contracts to do the transactions or rather how the existing applications have utilized these features in their research components.

Chapter 3, Methodology describes regarding the selection of the experimental environment through tracing and analysis. Therefore, this section of the research describes the proposed approach followed by the experimental platform from which the data has been collected, as well as the overview of the dataset that is collected and analyzing methodology. And also, it explains which crypto currencies are used in research, and how the decentralized applications work along with the concept of Blockchain. Comparison between each crypto currency which is available and testing methodology are also further explained in the chapter.

Chapter 4, Analysis & Results presents experimental set-up, test observations and results acquired by the executions of various methodologies and comparing them with each other methodology. Furthermore, it explores a benchmark analysis of results obtained by the dataset.

Chapter 5, Conclusion and Future Works summarizes research and highlights the new directions expected for future works, where more efforts should be taken with the aim of enhancing the accuracy and efficiency of this research

Chapter 2 – Literature Review

2.1 Introduction to the chapter

The first part of this chapter focuses on the overview of the research problem which the author is trying to resolve and the initiatives he has taken. The second part of this chapter explains the problem overview where the author explains the problem in detail, and he analyzes it furthermore. It also consists of how the author ended up choosing this research area, in order to solve this certain community problem which is vastly being faced by many people. In the third chapter it explains the problem domain, where the author explains the technical jargons which he is willing to use, and the possible alternatives which could've been utilized otherwise. Furthermore, he also discusses the pros and cons of using those technologies in order to make sure that he has chosen the best set of technology stack. The final two topics elaborates more on the existing applications which are out there, that have been researched and implemented in various other domains using different technologies. The author has pulled in details from various sources such as research papers, thesis' etc., in order to justify the problem statement.

2.2 Problem Overview

The problem which I'm trying to resolve here is to avoid users of various applications, from relying on the third-party companies or rather organizations in order to utilize the services which those applications provide. In other words, any mobile or web application which are out there in the planet, for them to provide their services, they indirectly request a user's confidential data, of which they might use it to sell those valuable data to the marketers and other larger organizations. For example, the social network applications such as Facebook, Twitter, Instagram etc. which are being used by the user daily are consuming the user's data without knowing themselves. While the user is using the application, the service providers can simply track the location of the user, and consume whatever the user is searching for, or even what are the related posts which he or she is looking at. So, there's a high chance of possibility for those companies to give out these confidential data to other third-party organizations for them to carry forward any marketing campaigns.

2.3 Problem Domain

This brings me to convey that, the above applications can be considered as centralized applications. Where the keyword centralized, illustrates that there is always a central governing body to create and overlook the rules, and the users are expected to adhere to the rules and follow according to them. As in when it comes to centralized network, the user data or the communication with the application will be done within a single point of network. This can be considered as a private hub, where only the organization which holds rights for that network, will

be able receive or send requests back and forth, to and from the application. Whereas a decentralized network relies on a host of computers which literally resides on a P2P network. It physically cannot work with a single computer or point-of-connection. Instead, it requires a slew of other computers to join in, in order to complete a specific task on the network.

The core issue which I'm addressing here is that, the mobile/web applications these days are centralized, and the user details are being exposed to the open world, where the user must willingly give away their personal data in order to utilize those services of the application. In order to prevent users from providing their data, I'm expressing a solution, as a proof of study for the concept of decentralized application, by creating a community-based application which is based on the concepts of decentralized and smart contracts. Since I have already mentioned about what decentralized does, over the existing centralized application, will go ahead and give what I'm trying to achieve using smart contracts. A smart contract is an agreement between two people in the form of computer code. They run on the blockchain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract processed by the blockchain, which means they can be sent automatically without a third party. This means there is no one to rely on. The transactions only happen when the conditions in the agreement are met — there is no third party, so there are no issues with trust.

2.4 Existing Applications

There are existing applications which were built based on blockchain and smart contracts. An author: "Emre Yavuz who has worked on towards secure e-voting using Ethereum blockchain [1], says that the blockchain with the smart contracts, emerges as a good candidate to use in developments of safer, cheaper, more secure, more transparent, and easier-to-use e-voting systems. In this work, they have implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. Android platform is also considered to allow voting for people who do not have an Ethereum wallet. After an election is held, eventually, the Ethereum blockchain will hold the records of ballots and votes. Users can submit their votes via an Android device or directly from their Ethereum wallets, and these transaction requests are handled with the consensus of every single Ethereum node. This consensus creates a transparent environment for e-voting. "

Furthermore, there is another existing application which is built based on smart contract and blockchain. This time it's related to car insurance where by using Smart Contracts and Sensors to Provide On-Demand Coverage. One of the authors: "Fabrizio Lamberti says that [2] Blockchains and sensors installed on a vehicle could be combined to semi automatically activate/deactivate car insurance coverage in an envisaged on-demand insurance scenario. They have presented a prototype that includes a mobile application (app) and a portable electronic device to be installed onboard. The mobile app lets the driver dynamically change the status of specific insurance coverage (in some cases, after pictures of the vehicle have been taken to attest to its conditions). Each modification and picture hash (a fixed-length alphanumeric summary of data

content) are saved on the blockchain within a smart contract to certify changes made as well as the vehicle's status. Sensors embedded in the electronic device are used to collect passengers' and the vehicle's data. Data are then used to automatically modify insurance coverage based on car/environment conditions and the preferences set. The proposed solution could help lower policy modification costs and limit insurance fraud."

The above are some of the applications which can be considered as proof of concepts, of the technical concepts such as blockchain and smart contract.

2.5 Approach

My personal approach towards this problem, is to create a community platform, based on smart contract and blockchain in order to build a public network where, the application will be implemented as entirely decentralized. The whole motivation behind this application, is to prove that there's no need to have a third-party organization managing the entire application inclusive of providing the services, purely based on the user's contribution towards the community. Once the user starts to contribute more, better the benefits he or she will get while using the application. Hence the basic outcome of this resolution would be that, there's no third party ruling the users, it's going to be the users who'll manage the privileges. As in, they must earn themselves points or credits by contributing to the community, so that they'll be able to utilize the features. Since this is an app related to train activities here in Sri Lanka, the public can view the current locations of the train which they are about to get in, or share the location while they're travelling, how many kms and how much time does it take to travel from one station to another etc.

Chapter 3 – Methodology

3.1 Overview

Methodology of the research begins from the selection of the experimental environment through tracing and methodology for analysis. Therefore, this section of the research proposal describes the proposed approach followed by the experimental platform from which the data has been collected, as well as the overview of the dataset that is collected and analyzing methodology

3.2 Research strategy

The research held with respect to this dissertation was an applied one, but not new. Rather, numerous pieces of previous academic research exist regarding the decentralized application which were built on top of block chain and smart contract for numerous sectors in the industry. Many research papers also justify that blockchains and smart contracts can be used as an effective option, when building decentralized applications. As such, the proposed research took the form of a new research but on an existing research subject.

3.3 Research method – Qualitative versus Quantitative techniques

In order to satisfy the objectives of the dissertation, a qualitative R&D was held. The main characteristic of qualitative research is that it is mostly appropriate for small samples, while its outcomes are not measurable and quantifiable (see table 3.1). Its basic advantage, which also constitutes its basic difference with quantitative research, is that it offers a complete description and analysis of a research subject, without limiting the scope of the research and the nature of participant's responses [3].

However, the effectiveness of qualitative research is heavily based on the skills and abilities of author, while the outcomes may not be perceived as reliable, because they mostly come from author's personal judgments and interpretations. Because it is more appropriate for small samples, it is also risky for the results of qualitative research to be perceived as reflecting the opinions of a wider population [4].

Qualitative research	Quantitative Research
The aim is a complete, detailed description.	The aim is to classify features, count them, and construct statistical models to explain what is observed.
Author may only know roughly in advance what he/she is looking for.	Author knows clearly in advance what he/she is looking for.
Recommended during earlier phases of research projects.	Recommended during latter phases of research projects.
The design emerges as the study unfolds.	All aspects of the study are carefully designed before data is collected.
Author is the data gathering instrument.	Author uses tools, such as questionnaires or equipment to collect numerical data.
Data is in the form of words, pictures or objects.	Data is in the form of numbers and statistics.
Subjective – individuals' interpretation of events is important., uses participant observation, in-depth interviews etc.	Objective: seeks precise measurement & analysis of target concepts, e.g., uses surveys, questionnaires etc.
Qualitative data is 'richer', time consuming, and less able to be generalized.	Quantitative data is more efficient, able to test hypotheses, but may miss contextual detail.
Author tends to become subjectively immersed in the subject matter.	Author tends to remain objectively separated from the subject matter.

Table 1: Features of Qualitative & Quantitative Research (Adapted from [5])

3.4 Research approach

The research approach that was followed for the purposes of this research was the inductive one. According to this approach, the author begins with specific observation, which are used to produce generalized theories and conclusions drawn from the research. The reasons for occupying the inductive approach was that it considers the context where research effort is active, while it is also most appropriate for small samples that produce qualitative data. However, the main weakness of the inductive approach is that it produces generalized theories and conclusions based only on a small number of observations, thereby the reliability of research results being under question [6].

3.5 Data Collection

Since this project is being implemented as a blockchain based decentralized application, it is highly necessary to collect the correct amount of data in order to carry forward with the application. At the end of the day, it's going to be the numbers or rather the data in this perspective, which the author will be willing to use and analyze. As a proof concept, the author is trying to develop a D-App which could help the public who're using the train as their public transport on a day to day basis. Hence the data for this application was gathered from the department of railway of Sri Lanka where they had the API developed to retrieve the details regarding the trains that travel to every single place, and the train schedules.

The API which was already created by ICTA in order to get the train schedules wasn't public for a developer to go ahead and utilize it. Hence the author had to contact the authorized personnel and get the necessary API details. Not only the schedule details, the prices of the tickets according to the class in which the passenger wanted to travel, also was acquired from the Railway Department. It differs destination to destination. The other major dataset which the author was trying to acquire, was the passenger details. Since it was quite hard to gather all the passenger details in person, the author had to generate random data in order to fill in the details for the usage of the application. The author also made sure that the passenger details were unique, so that there won't be any duplicates which could affect the dataset when using it.

3.6 Data Preparation

The author did not get any sort of information, or rather feedbacks from the public via any questionnaires, since the information which we're talking about is related to only the people who use train as their daily travel need. Hence it was highly necessary to go directly to those people and get their feedback on the application which the author is trying to build. So the author personally went and met some of the public who were travelling on the train and asked a

few general questions such as, how often does the passenger travel by train, how hard is it to know the exact time of the train departure/arrival, what are the possibilities of the train getting delayed, is it possible for the passenger to know where the train is located at a given moment? The author went ahead and collected all the answers from the passengers, which is vital for analysis and for the betterment of the application.

When the author started analyzing the result set which he got from the public, most of them have the issue of trains getting delayed and them now knowing about it. So, in order to elaborate on this, there are people who leave home early in order to make into the station and catch the train on time, since it'll be crowded. If the train is going to arrive late, they'll always have the luxury of leaving on time, rather than spending their valuable time at the station waiting for the train for hours. Another issue which the public were facing was that, whenever a train gets halted due to some track issues, or due to signal issues or it could be even due to an accident. Even though all this happens, there's no way the public would be aware of this. Hence it would be great, whenever either any of the above happens, to send out an alert to the passengers who're waiting for that train, so that they'll be aware of it and they don't have to panic due to the delay. It's going to be also helpful to the passengers, if they can get the maximum usage out from this research application, such as knowing the exact location of the train at any given moment, and how long would it take to reach their station. Author also emphasizes that this should be a completely community app, where the users themselves contribute to the app, and they get something in return for doing so.

So, the selected data set was used in the D-app for the implementation purposes. None of the data was reformed or preprocessed or rather modified. It is being used as it was gathered. Since most of the feedback or rather comments which were taken from the public were handwritten and recorded, hence the author is unable to provide an analytical breakdown of what the users are thinking about the application. Therefore, the author is trying to elaborate on what the public thinks about having a community app from which they can gain useful information and their recommendations on what is already there, such as the train schedule apps. The author is pretty much confident on what he's implementing, as it is different from the already existing applications in this domain, and it'll be vastly useful for the community as many of them here in Sri Lanka use train as their main transport.

3.7 Data Analysis

Content analysis was used to analyze the data which was gathered from personal interviews. According to Moore & McCabe [7], this is the type of research whereby data gathered is categorized in themes and sub-themes, to be able to be comparable. A main advantage of content analysis is that it helps in data collected being reduced and simplified, while at the same time producing results that may then measure using quantitative techniques. Moreover, content analysis gives the ability to researchers to structure the qualitative data collected in a way that satisfies the accomplishment of research objectives. However, human error is highly involved in content analysis, since there is the risk for researchers to misinterpret the data gathered, thereby generating false and unreliable conclusions [8].

Chapter 4 – Project Management

4.1 Chapter Overview

Previous chapter discussed about the literature review of the project. This chapter will be focusing on the project management process of the proposed system. This starts with finding out a proper project management methodology. Then the chapter moves on to talk about the time and resource allocation. The next chapter will be discussing about the project risks and focuses on the selection of development methodology for this system.

4.2 Project Management Methodology

The PRINCE2 management technology is being used for the proposed system due to the following reasons. This project's scope is big enough so that it takes immense time to research. Important objective of the project is to give a quality output. For this proposed system, time management and quality management are hard to achieve due to the depth of scope. After comparing with the other project management methodologies, PRINCE2 was selected because it's used widely and it's easy to handle time management.

4.3 Development Methodology

To develop and deliver a quality project with low cost and within an actual time period, a proper development methodology is crucial. Due to the above reason, the author has analyzed various kinds of development methodologies such as code and fix, waterfall, Rup, Agile and spiral with mentioning all their characteristics, advantages and disadvantages in order to choose a proper methodology for this project. The following image (Figure 3.1) shows the comparison of the available development methodologies.

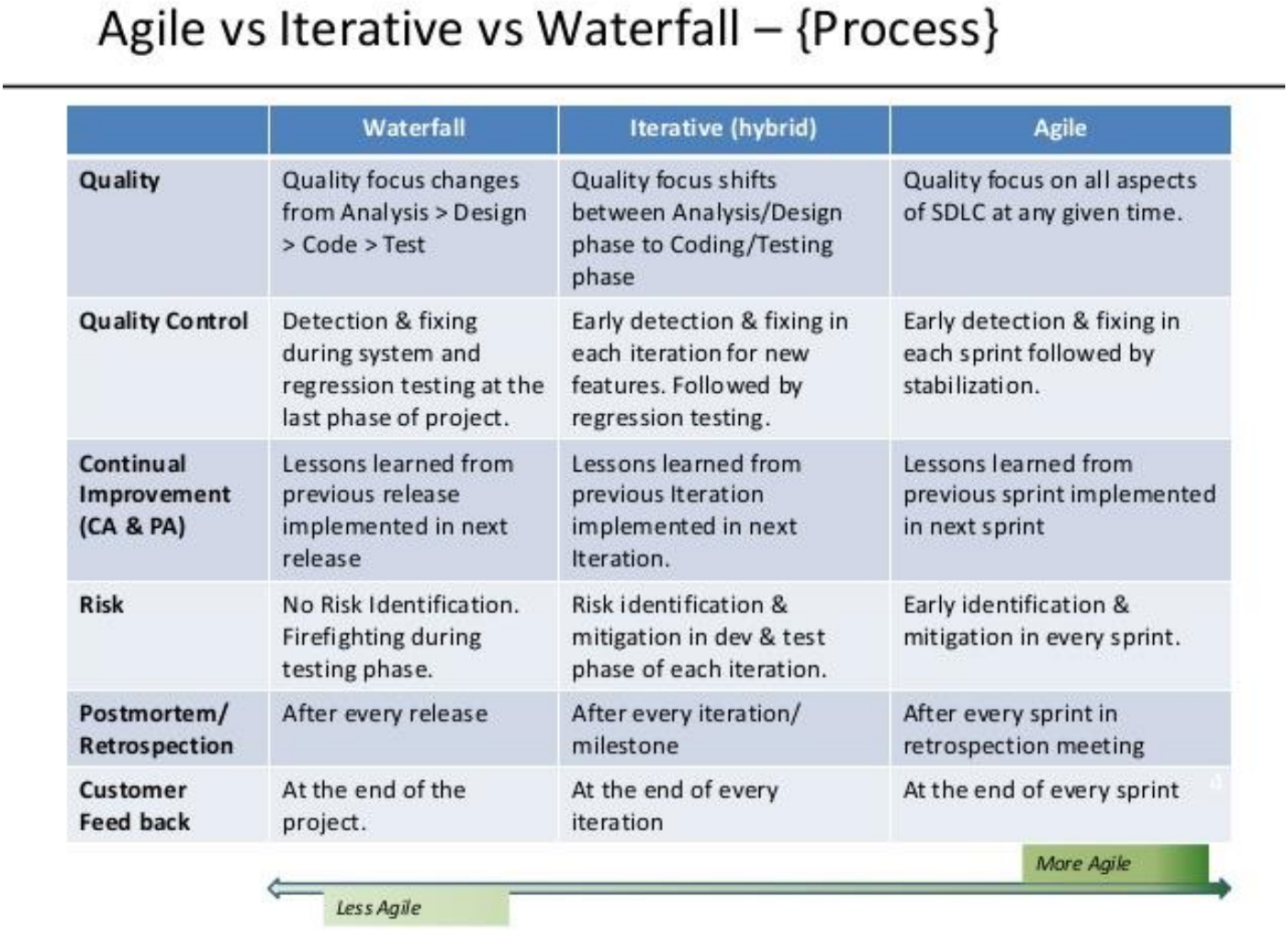

Figure 1 – Adapted from [19]

4.4 Research Methodology

There are two categories of research methodologies such as inductive researching and deductive researching. In an inductive perspective to research, a researcher starts gathering data which is necessary to his or her topic of interest. Deductive approach is aimed at proving and testing a proposal. Deductive research methodology was chosen for this project in order to perform testing and evaluation with the suggestions of the domain experts as mentioned in the introduction chapter.

4.5 Chapter Summary

This chapter focused on project management which helped this proposed system to complete successfully. This chapter started with explaining about the project management methodologies where, PRINCE 2 was selected since it's widely used and easy to handle time management factor. Then the chapter moved on to talk about the time allocation which is one of the main tasks of the project. There after the chapter moved on to explain about the development methodologies where various kinds of development methodologies were compared, and finally spiral development methodology was selected. Finally, this phase discussed about the research methodology where deductive research methodology was selected among both inductive research and deductive research.

Chapter 5 – Implementation

5.1 Chapter Overview

The previous chapter discusses about the methodology which is being used in the proposed system where as this chapter will be focusing on the implementation of the proposed Blockchain based decentralized app. This phase will be discussing about different kinds of technologies, frameworks, APIs and development environments which were used to implement the proposed system. This will be also discussing the problems which were occurred during the implementation.

5.2 High-level Diagram of the functionalities

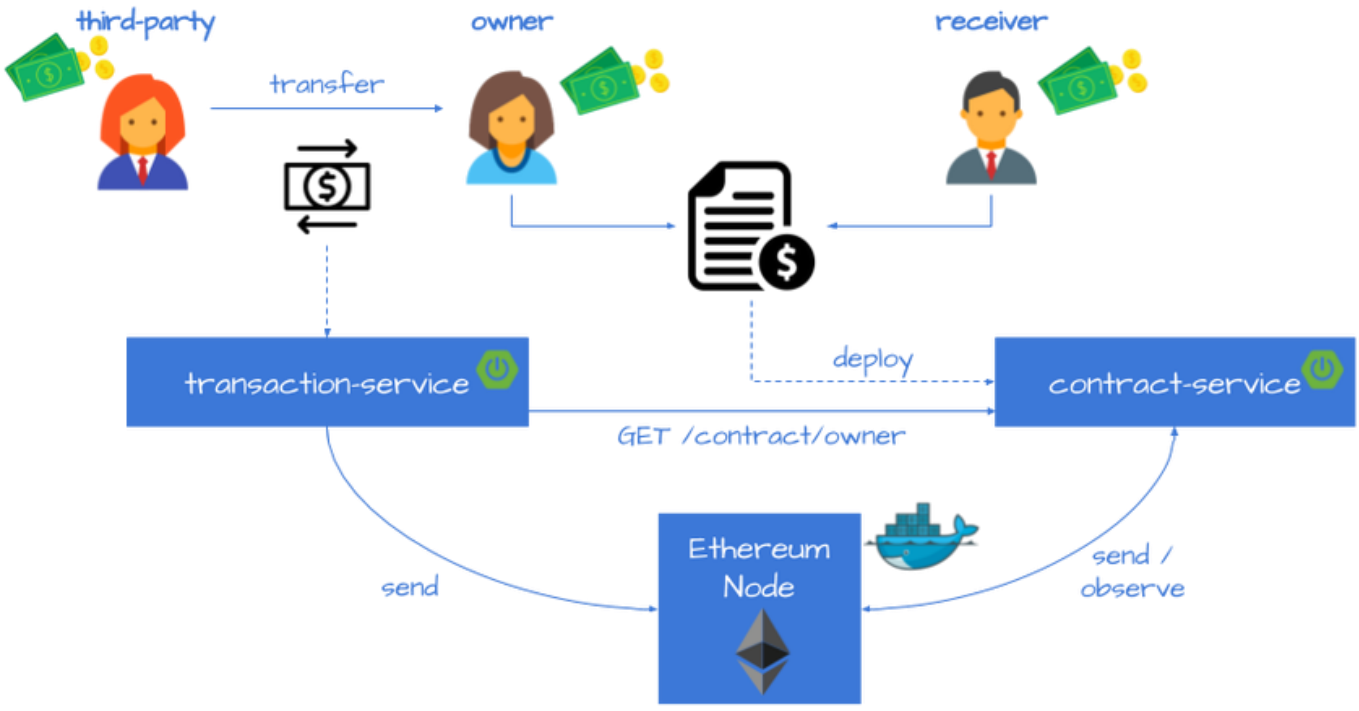

Figure 2 [20]

A DAPP (Decentralized Application) consists of back-end code that runs on a decentralized peer-to-peer network. A DAPP can also have a user interface, created by front end code that makes calls to the back end. DAPPs do not require a central authority to function: they allow for direct interaction between users and providers.

DAPPs often have the following characteristics:

- They run on the blockchain
- Their code is made open-source operates autonomously without any person or group controlling the majority of tokens
- They generate DAPP tokens to provide value to their contributing nodes
- Users are granted access to them in exchange for tokens
- Miners are rewarded with tokens when they successfully contribute to the ecosystem

Users can transact with one another on a blockchain network, using its intrinsic currency. These DAPPs usually have their own blockchains, and we often refer to them as cryptocurrencies (such as Bitcoin).

DAPPs essentially allow all the back-end code and data to be decentralized, and hence immutable and tamperproof. Considering the decentralized nature of these applications coupled with the mechanisms that secure blockchain data, DAPPs have the potential to unlock a diverse array of use cases.

A few benefits of creating a DAPP rather than a normal application include:

• Payment processing: no need to integrate with a fiat payment provider to accept funds from users, as users can transact directly using cryptocurrencies

• User credentials: using a system of public and private keys, users can transact and bind their user sessions and metadata easily and with varying degrees of anonymity, negating the need for lengthy sign-up or registration processes

• Trust and auditability: open-source DAPP code is accessible and understandable to savvy users. This transparency and the inherent security of the enclosed data generates confidence in the applications. A public record on the blockchain also makes transaction information easy to audit by users or third-parties

5.3 Technical Information

5.3.1 System & Software Design

The system was developed using a hybrid of the “waterfall” model and the evolutionary development model as defined by Sommerville (1996) [9]. This meant that the benefits of the structured approach offered by the waterfall model could be combined with the prototype approach used in the evolutionary development model. The waterfall model starts off with the definition of requirements (in this case the output of the development module of Hubbard’s

(1996) [10]. This feeds into the system and software design phase, which establishes an overall system architecture and involves representing the software system functions in a form that can be converted into executable programs.

Integration and system testing refer to the integration of the programs as a system and the testing of the complete system. Operation and maintenance occur when the system is installed and put into use. Maintenance involves correcting errors (and can also cover improving and enhancing the system). In evolutionary development an initial implementation is developed, shown to the user and refined until an adequate system has been developed. Specification, development and validation are not separate activities, they happen concurrently with feedback between activities. The software development process of this project used a combination of both models. It followed the waterfall model in so far as it started with a set of requirements as outlined earlier. The overall system and software were designed based on these requirements. The system was then implemented, and each program or part of the system was individually tested.

5.3.2 The Software Design Methodologies

Many software development projects have been known to incur extensive and costly design errors. The most expansive errors are often introduced early in the development process. This underscores the need for better requirement definition and software de sign methodology. Software design is an important activity as it determines how the whole software development task would proceed including the system maintenance. The design of software is essentially a skill, but it usually requires a structure which will provide a guide or a methodology for this task. A methodology can be defined as the underlying principles and rules that govern a system. A method can be defined as a systematic procedure for a set of activities. Thus, from these definitions, a methodology will encompass the methods used within the methodology. Different methodologies can support work in different phases of the system life cycle, for example, planning, analysis, design and programming, testing and implementation. Svoboda (1990) developed the idea of a methodology further by proposing that there should be at least four components:

- a conceptual model of constructs essential to the problem,
- a set of procedure suggesting the direction and order to proceed,
- a series of guidelines identifying things to be avoided, and
- a collection of evaluation criteria for assessing the quality of the product.

The conceptual model is needed to direct or guide the designers to the relevant aspects of the system. The set of procedure provides the designer a systematic and logical set of activities to

begin the design task. The evaluation criteria provide an objective measurement of the work done against some established standard or specifications.

A software design methodology can be structured as comprising of the software design process component and the software design representation or diagrammatic component. The process component is based on the basic principles established in the methodology while the representation component is the "blueprint" from which the code for the software will be built. It should be noted, that in practice, the design methodology is often constrained by existing hardware configuration, the implementation language, the existing file and data structures and the existing company practices, all of which would limit the solution space available to develop the software. The evolution of each software design needs to be meticulously recorded or diagramed, including the basis for choices made, for future walk-throughs and maintenance.

Level Oriented Design (LOD) was chosen as the design methodology for the proposed system. In the level-oriented design approach, there are two general or broad strategies that can be used. The first strategy starts with a general definition of a solution to the problem then through a step-by-step process produce a detailed solution (this is called Stepwise Refinement). This is basically dependent on the system requirements and is a top-down process. The other strategy is to start with a basic solution to the problem and through a process of modeling the problem, build up or extend the solution by adding additional features.

The top-down process starts at the top level and by functional decomposition, breaks down the system into smaller functional modules. Smaller modules are more readily analyzed, easier to design and code. But, inherent in the top-down process is the requirement that there must be a complete understanding of the problem or system at hand. Otherwise, it could lead to extensive redesign later. The top-down process also is dependent on decisions made at the early stages to determine the design structure. Different decisions made at the early stage will result in different design structures. Functional decomposition is an iterative "break down" process called stepwise refinement, where each level is decomposed to a more detailed lower level. Thus, at each decomposition, there must be a way to determine if further decomposition is needed or necessary, that is, if the atomic level has been achieved. There are no inherent procedure or guidelines for this. There is also a possibility of duplication if stepwise refinement is not done carefully or "correctly"; this will occur toward the end of the process, that is, at the lower levels. This can be costly, especially if there are many different designers or programming teams working on a single system. As a result, the top-down process is often used in the initial phase of the design process to break down the different components or modules of a system. The top-down process has also been used as a preliminary step in the other design methodologies. Once

the modules of the system have been determined, they can be divided amongst the different designers or design teams [21].

5.3.3 Selection of Programming Language

This section discusses about which language is being used to develop this application. The selection of the program language wasn't hard enough, since there are only a handful of languages which you can work with, such as C++, Java, Python, Simplicity and Solidity. After the author analyzed all the possibilities and the effectiveness of the languages, when dealing with D-apps along with Blockchain and Smart contracts, it has been proven and justified that Solidity is being used by most of the developers. Solidity is utilized as a contract-oriented, high-level language, in order to implement smart contracts which are based on Blockchain. The technical details regarding Smart contract and Blockchain will be discussed in detail below. This language is basically influenced by C++, Python and JavaScript and is well designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features. As you will see, it is possible to create contracts for voting, crowdfunding, blind auctions, multi-signature wallets and more [11].

5.3.4 Tools and Technologies Used

There are a quite few technologies which have been used in this research component such as Blockchain, Smart contract and other open source tools like Remix, Solidity, Ganache etc. The author had to pick some of these tools among the other, which are out there in the paradigm and all these tools were picked based on the recommendation given to each and individual tool and technology. The author also took into consider that, he must follow all the best practices which are out there, in order to make this implementation as a success.

Blockchain:

At its most basic level, blockchain is generally a group of blocks, but not in the traditional sense of those words. When we say the words block and chain in this context, we are talking about digital information such as a block being stored within a public database.

Blocks on the blockchain are made up of digital pieces of information. Specifically, they have three parts [12]:

1. Blocks persists data about the transactions that are made such as the date, time, and the amount of your most recent purchase.

2. Blocks persists data about who involves with the transactions. Instead of using your actual name, the purchase is recorded without any identifying information using a distinct digital signature which could be considered as of like a username.

3. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a “hash” that allows us to tell it apart from every other block. Let’s say you made your splurge purchase on Amazon, but while it’s in transit, you decide you just can’t resist and need a second one. Even though the details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

How Blockchain works?

Initially if two parties wanted to make any sort of transactions, there aren’t any middle man or rather any sort of banks to take control of this, since it’s entirely decentralized. All the transactions are considered as blocks, where it’ll store all the blocks in a chain. Every single transaction will be broadcasted or rather notified to all the peers who’re in the blockchain network. Once they’re being notified with the details of the transactions, they must approve the transaction for it to be considered as valid. Thereafter if the transaction is proven to be valid, it will be added to a chain of blocks which is ideally named as Blockchain, and the cash would be transacted between two parties.

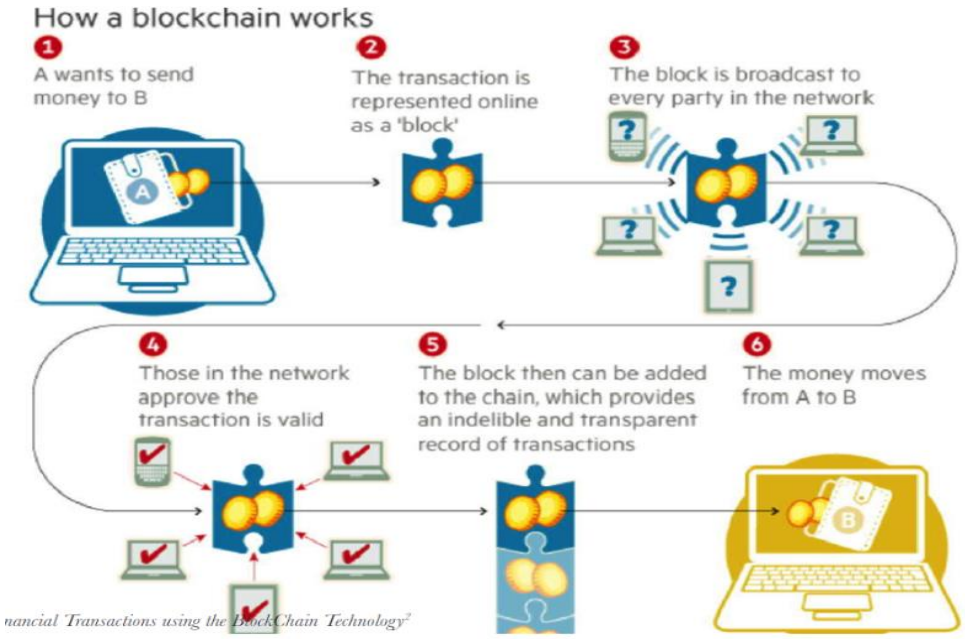

Figure – 2 (Adapted from [13])

Smart Contract:

Max Raskin has stated about a smart contract as [14] “A new technology called “smart contracts” has emerged. What makes these legal agreements innovative is that their execution is made automatic through the use of computers. This Article examines smart contracts from a legal perspective. Specifically, this Article explains smart contracts’ operation and place in existing contract law. It introduces a distinction between strong and weak smart contracts, as defined by the costs of their revocation and modification. The article concludes that smart contracts are simply a new form of preemptive self - help that should not be discouraged by the legislatures or courts. While certain unconscionable examples of strong smart contracts may need to be policed, judges and policymakers should foster a climate that treats smart contracts as another form of more traditional agreements.”

A smart contract is basically known as a crypto contract, which is a computer program that instantly controls the transferal of digital currencies or assets among groups under some sort of conditions. A smart contract does not only determine the conditions and sanctions which are related to an agreement in the same way that a traditional contract does, but it can also automatically enforce those obligations. It does this by taking in information as input, assigning a value to that input through the rules set out in the contract and executing the actions required by those contractual clauses -- for example, determining whether an asset should go to one person or should be returned to the other person from whom the asset originated. These contracts are stored on blockchain technology, a decentralized ledger that also underpins bitcoin and other cryptocurrencies.

What smart contracts do:

Smart contracts are complex, and their potential goes beyond the simple transfer of assets -- they can execute transactions in a wide range of fields, from legal processes to insurance premiums to crowdfunding agreements to financial derivatives. Smart contracts have the potential to disintermediate the legal and financial fields; by simplifying and automating routine and repetitive processes for which people currently pay lawyers and banks sizable fees. The role of lawyers could also shift in the future as smart contracts gain traction in areas from adjudicating traditional legal contracts to producing customizable smart contract templates. Additionally, smart contracts' ability not only to automate processes, but also to control behavior, as well as their potential with real-time auditing and risk assessments, can be beneficial to compliance.

How Smart contract works?

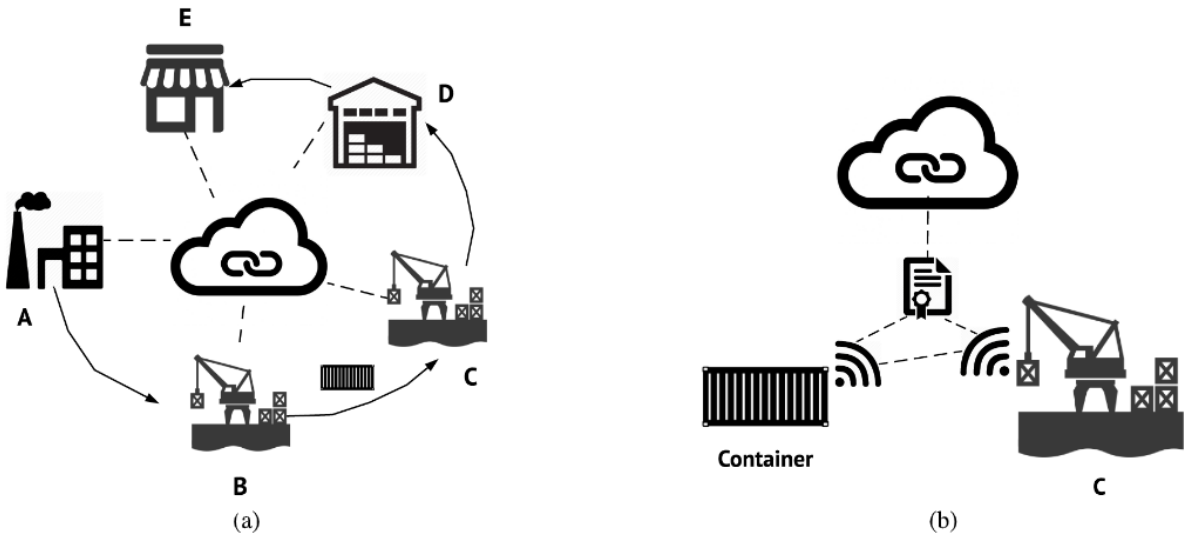

Figure- 3(Adapted from [15])

Figure 2: An asset tracking example using smart contracts and IoT. In Fig. 4a (left) a container leaves the manufacturing plant (A), reaches the neighboring port (B) via railway, gets transported to the destination port (C), and then to the distributor's facilities (D), until it reaches the retailer's site (E). In Fig. 4b (right), we focus on the B-C stage. The carrier of the container performs a handshake with the dock at the destination port (C) to confirm that the container is delivered to the expected location. Once that handshake is completed, it posts to a smart contract to sign the delivery. The destination port follows along to confirm reception. If the node at C does not post to the contract within an acceptable timeframe, the shipping carrier will know and can initiate an investigation on the spot [15].

Smart contract is an entirely new technology. Even though, consisting a lot of potential, it is still can be vulnerable to problems as it's a new technology domain. As an example, the piece of code snippet which constructs the contract should be accurate and shouldn't consist any sort of bugs. This can guide to issues and, at times, these sorts of bugs could be fully utilized by the scammers. Furthermore, the newness of the technology stack still brings a whole lot of questions into the table. How will the state's administration decide to modulate such contracts? How will the taxes be levied on these contracts? What happens when the contract does not get any privilege to the subject of the consensus, or something unforeseen happens to it? If this was to occur when a conventional contract was created, it could be revoked in court, but then the Blockchain will make the contract achieve no matter what, due to the policy. Nonetheless, most of these issues subsist only because of the reason, how new the smart contracts are as a

technology. With such promise, the technology will surely be perfected over time. Undoubtedly, smart contracts are about to become the integral part of our society.

What is Ethereum?

To put it simply, Ethereum is looked upon as an open software platform which is completely based on the blockchain technology which lets the programmers to write and deploy decentralized applications. As Dejan Vujičić et al. mentioned Ethereum was introduced in Vitalik Buterin's paper [29] and addressed several limitations of the Bitcoin's scripting language. The main contributions are full Turing-completeness, meaning that Ethereum supports all types of computations, including loops. Then Ethereum supports the state of the transaction, as well as several other improvements over the blockchain structure. Ethereum represents a blockchain with a built-in Turing-complete programming language. It provides an abstract layer enabling anyone to create their own rules for ownership, formats of transactions, and state transition functions. This is done by involving smart contracts, a set of cryptographic rules that are executed only if certain conditions are met. The consensus in the Ethereum network is based on modified GHOST protocol. It is created to tackle the issue of stale blocks in the network. The stale blocks can occur if one group of miners combined in a mining pool has more computing power than the others, meaning that the blocks from the first pool will contribute more to the network, thus creating the centralization issue. GHOST protocol includes those stale blocks into calculations of the longest chain. The centralization problem is removed through providing block rewards to stales, where the stale block receives 87.5% of the reward, and the nephew of that stale block receives the remaining 12.5% of the reward. In this way, the miners are still rewarded even if their block didn't become the part of the main blockchain (those blocks are called uncles). Ethereum uses the modification of the GHOST protocol which includes uncles up to seven generations [16].

Moreover, the whitepaper of Ethereum explains the fact that, The Ethereum blockchain is in many ways like the Bitcoin blockchain, although it does have some differences. The main difference between Ethereum and Bitcoin about the blockchain architecture is that, unlike Bitcoin, Ethereum blocks contains a copy of both the transaction list and the most recent state. Aside from that, two other values, the block number and the difficulty, are also stored in the block. The approach may seem highly inefficient at first glance, because it needs to store the entire state with each block, but efficiency should be comparable to that of Bitcoin. The reason is that the state is stored in the tree structure, and after every block only a small part of the tree needs to be changed. Thus, in general, between two adjacent blocks most of the trees could be the same, and therefore the data can be stored once and referenced twice using pointers (i.e. hashes of subtrees) [17].

How Ethereum and Bitcoin function?

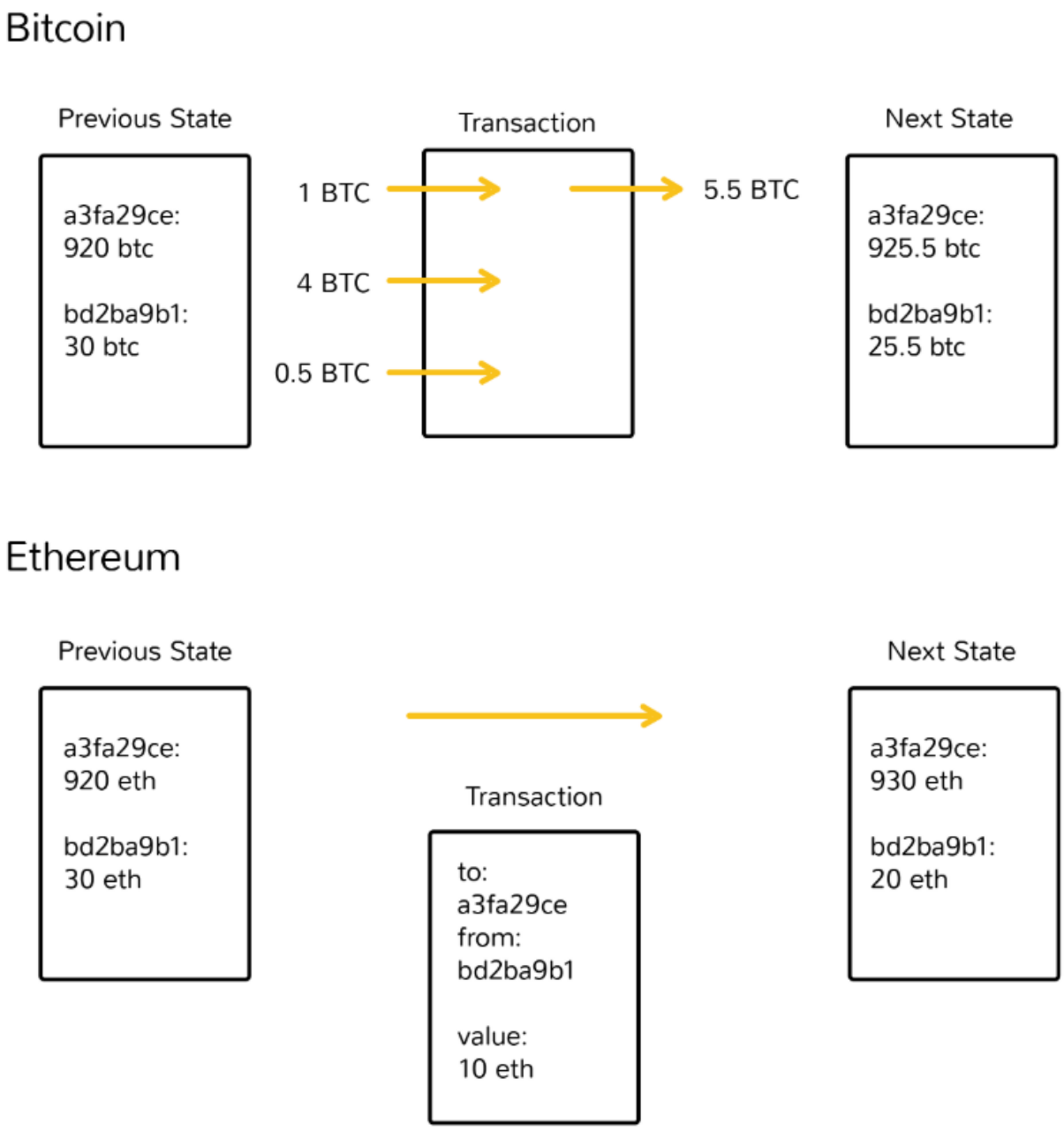

Figure 4 – Adapted from [18]

Chapter 6 – Evaluation & Test

6.1 Introduction

The chapter presents testing and evaluation of the entire work, categorizing it into two parts. First part deals with the self-assessment of the relevant domains such as development methodology adopted and envisaged aims, objectives and deliverables viz-a-vis results achieved at the end of project. The second part deals with evaluation with respect to GUI and application performance, while being inserted with real data. Actions taken to address these observations have also been discussed in these sections. Some of observations raised by project supervisor after first iteration also become part of this chapter.

6.2 Development Methodology

Waterfall methodology had been adopted for the project, with allowance to refer to previous development stages in case of any critical feedback and subsequent iteration, as discussed. The modified iterative waterfall model proved to be a good choice, since it broke the project into small, definite and manageable stages, with each stage required to be completed, documented and validated (informally by project supervisor), before next one can be initiated. Moreover, the strategy also helped in managing two iterations within limited available time, with first one focusing upon the application logic and mathematical model, whereas the second one improving upon GUI functionality and logic refinement, based on user evaluation. All in all, the selected methodology provided clear steps to be followed, while moving back and forth between different development stages and ensured timely completion of the project according to initial milestones and timelines.

6.3 Project Aim, Objectives & Deliverables

The aim of the project was to develop a decentralized application, by creating a community-based application which is based on the concepts of decentralized, smart contracts and blockchain. The intention was to avoid the problem of information overload, while offering robust decision-making process based on reliable sources of guidance. The aim was accomplished by meeting all objectives and deliverables set out at the start of the project.

6.4 Evaluation Approach

The evaluation approach for this project will be taken by conducting various methods such as experiment based (if possible) and mainly it will be opinion & interview based. So, in other words, before even the application is being deployed, there will be a questionnaire or a public survey which would consume important details from public who use train as their public transport in their day to day life. The questionnaire/survey would contain, core questions such as

how often they check for train timetables, how often do they check where a particular train is right now, on a scale of rating how much they would like to be active in such community to help others and provide valuable information. The result set of these questions would provide some handful of information, which could be utilized to enhance the application further, or go back and revert any functionalities which aren't useful.

The ways of conducting the survey would be, by interviewing some of the public during the travel by asking them questions, then sending around a survey in the social media (which might capture people who do and don't travel by train as their daily transport) and also getting the feedback from the industrial experts in order to make sure and verify the reason and motive behind in developing the community platform. As a result, the expected outcome should be that the end users must feel that, they're contributing so much to the community and they should also feel that they'll be rewarded for what they have done. As an experiment, the initial version of the application could be rolled out for the public usage as a free version and can evaluate how good/bad the users have used and reviewed the application. Based on the comments provided by the users, should enhance the application so that an updated version could be rolled out for the users back again. Another experiment could be, deploy the application on a sample test device, and move along with passengers who travel by train and ask them to give it a test run and explain them the features and the motive behind by using the application in detail.

6.5 Tools/Techniques/Data Sets

The tools which will be used for this application are Ganache, which is being used as a test Blockchain network, Remix which is an online developing tool for Solidity and Metamask which allows to run Ethereum d-Apps within the browser itself, without running a full Ethereum node. Currently the test data set will be extracted from the SriLankan Railway Train Schedule API plus a random generated dataset will be used for customer related information.

Ganache:

Ganache, which is earlier known as Testrpc, is considered as a virtual blockchain which establishes 10 Ethereum addresses by default, complete with private keys and all, and fore-loads them with 100 reproduced Ether each. There is no mining per-se with Ganache alternatively, it instantly guarantees any transaction which is forthcoming its way. This makes repetitive development feasible. The unit tests can be written for the code which executes on this simulated blockchain, deploy smart contracts, play around, call functions, and then tear it all down for further simulation or new tests, returning all addresses to their initial state of 100 Ether. Ganache comes in two flavors: CLI and UI. You can decide which one you want to download on their download page. My recommendation is the UI version purely because of simplicity. When you fire it up, it will default to a certain port and IP address.

Once you run Ganache, you should see a screen like this:

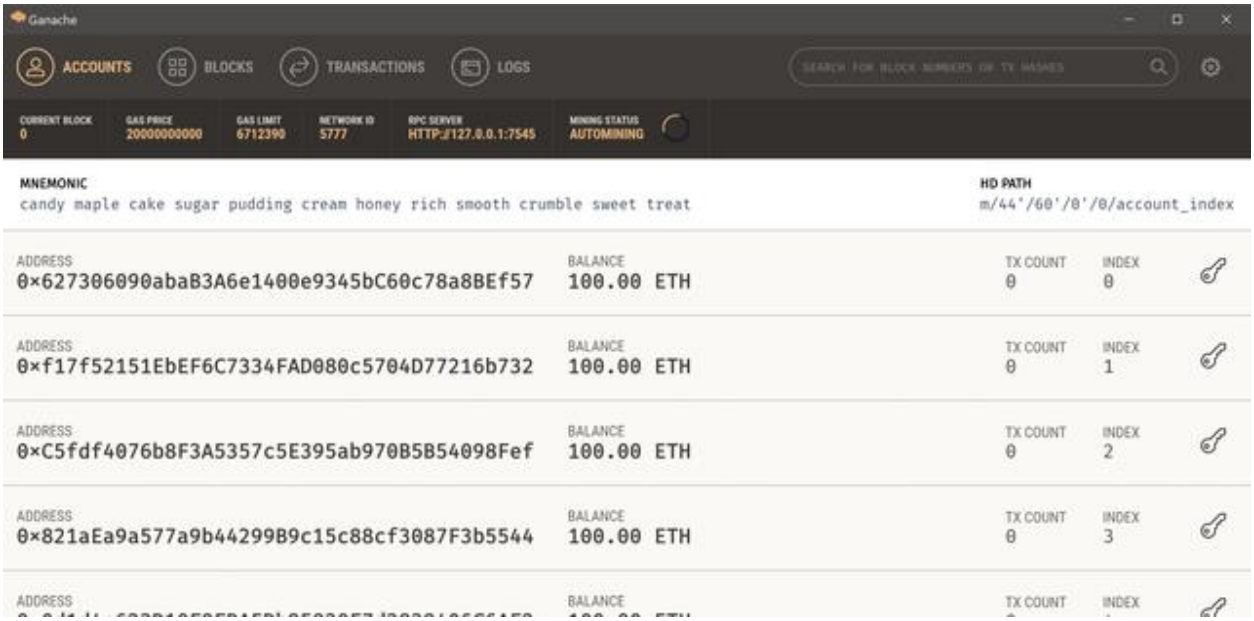

Figure 5 – Adapted from [25]

By executing Ganache, the author has constructively had his own Ethereum node up and running. It's a virtual node, sure, but it's used the same way as any real node and that means you can connect to it with wallets like MyEtherWallet or even browser wallets like MetaMask [25].

Transaction Section

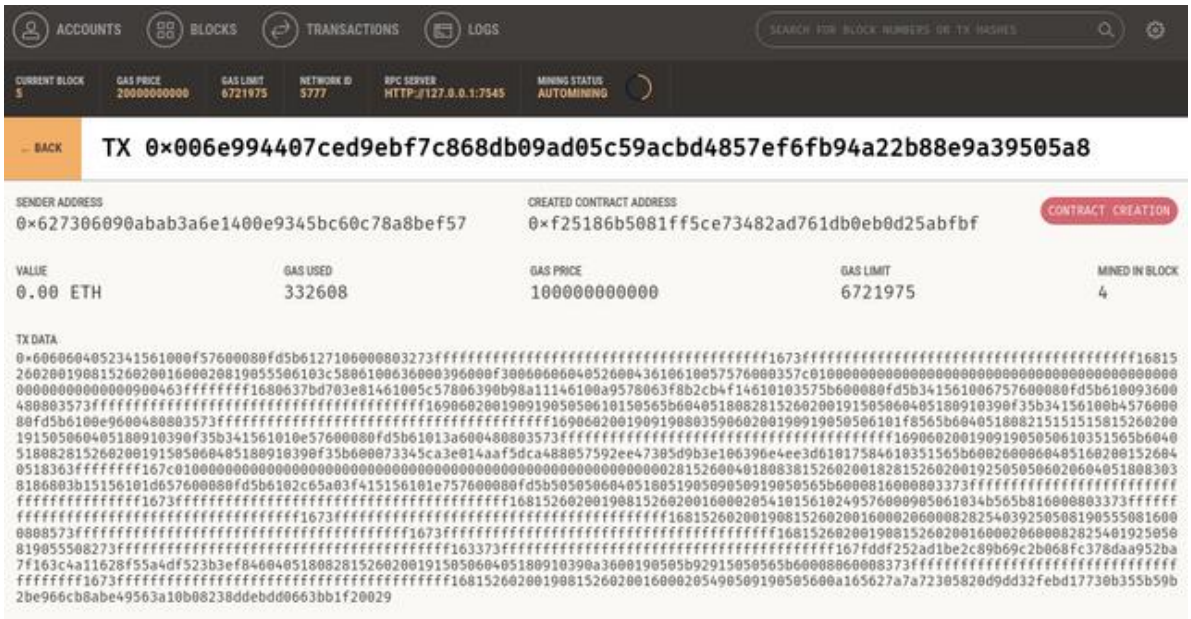

Figure 6 – Adapted from [26]

Metamask:

MetaMask is a connection that enables the author to visit the distributed web in the browser. It also authorizes the author to execute the Ethereum dApps right in the browser without running a complete Ethereum node, as quoted in their official website. MetaMask is a straightforward browser extension that can execute on various browsers and can be installed easily. Once it's installed, the author can generate a new Ethereum account in order to send and receive Ether and to execute the decentralized applications. Once producing an account, there will be a list of 12 words that can be used to retrieve your account when you forget your password. This must be saved somewhere safe where anyone would be able to visible it.

The real breakthrough comes with the tool's ability to specify which Ethereum node to send these requests to. This is a very important aspect because it allows users to enjoy Ethereum without the need of downloading over 10+GB of blockchain on to their hard drives just to make one small transaction.

Once the Ethereum wallet is available, the author will be able to utilize the core network, which will use real ethers that cost real money, or try out some of the dApps on the test networks.

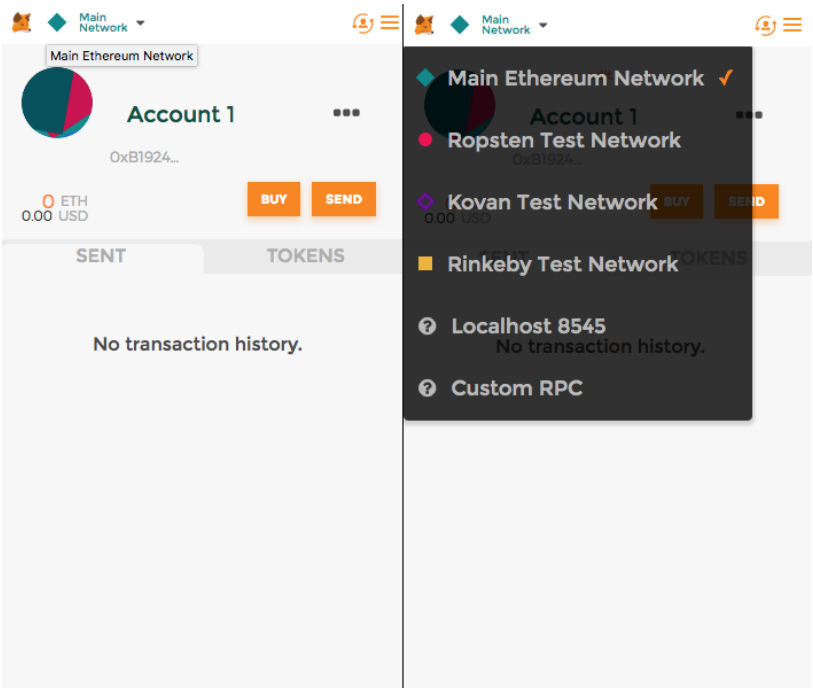

Figure 7 – Adapted from [27]

Sending and receiving Ether:

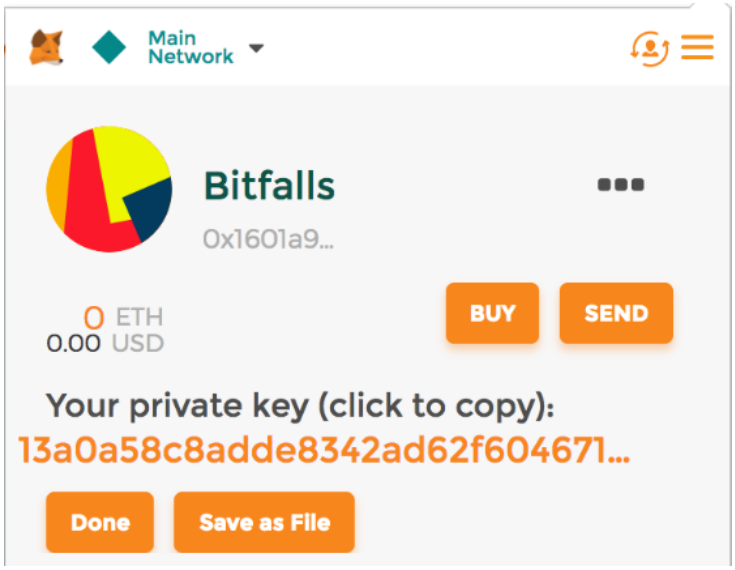

Figure 8 – Adapted from [28]

Solidity:

Solidity is an uncontaminated programming language which is indigenous to Ethereum, the second largest cryptocurrency by market capitalization, which was originally announced in 2015. Ethereum is not only a cryptocurrency competent of preserving value or making transactions, but an entirely ripened platform for creating what's known as a smart contract.

The Solidity language is one of numerous programming languages that can be compiled into Ethereum Virtual Machine (EVM) bytecode. Every programming language might have various compiler tools, but they all do the same thing, which is to precipitate EVM machine-level bytecode to be execute on the Ethereum nodes, for transactions.

Solidity uses a large number of programming conceptualizations that subsist in other languages. As for an example, Solidity has variables, functions, classes, arithmetic operations, string manipulation, and so on. While in a language like C, a programmer would likely create some form of a "main" function, like "int main(arg1, arg2) { //code }", Solidity works with a "contract" that is created in a similar manner [30].

```
pragma solidity >=0.5.0 <0.7.0;

contract Coin {
    // The keyword "public" makes those variables
    // easily readable from outside.
    address public minter;
    mapping (address => uint) public balances;

    // Events allow light clients to react to
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    constructor() public {
        minter = msg.sender;
    }

    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount < 1e60);
        balances[receiver] += amount;
    }
```

Figure 9 – Adapted from [29]

Remix:

Remix, which was earlier known as the Browser Solidity, is a web browser-based IDE that enables the author to construct Solidity smart contracts, then deploy and run the smart contract. The author can execute Remix from the web browser itself by traversing to https://ethereum.github.io/browser-solidity/, or by installing and running in the author's local machine [31].

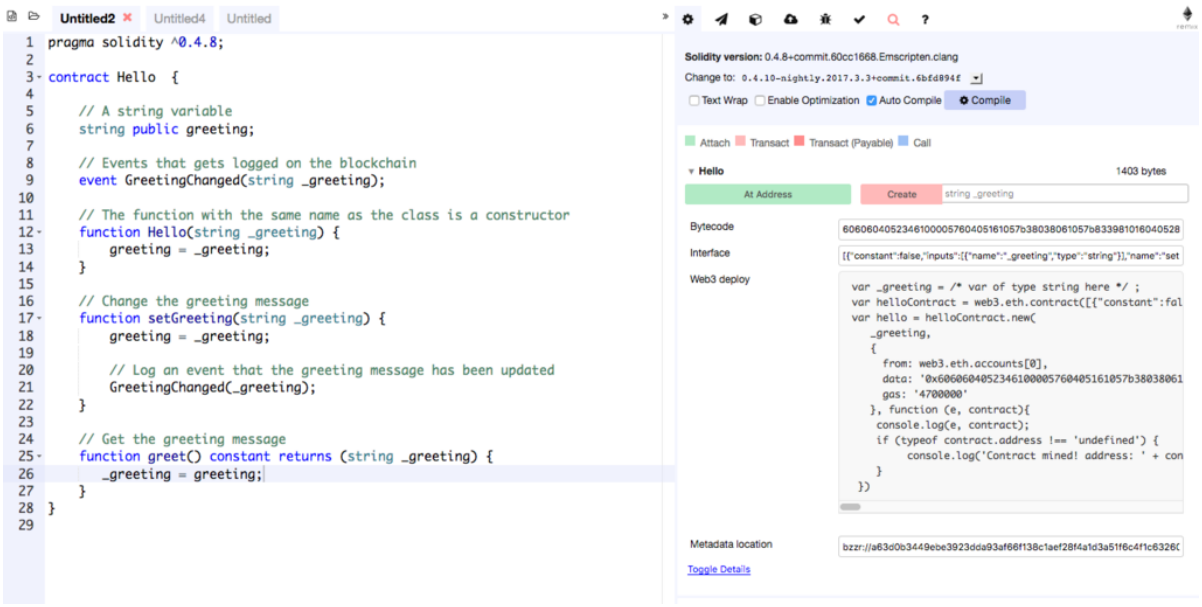

Figure 10 – Adapted from [30]

6.6 Test Plan

Once the evaluation is successfully done, test methodologies will be applied to make sure that the application runs without any flaws. In order to justify the approach which, the author has followed, multiple testing methodologies will be used to reduce or eliminate all the erroneous functionalities.

6.7 Testing Criteria

The four criteria for the success of a project are:

- The software must meet all the quality requirements.
- The software must be developed within the time frame.
- The software must be developed within the budget.
- The relations amongst the team members should be cordial during the project execution and after the project is completed.

Quality

The most important requirement of a software product is that it should meet the requirements of the customer. In addition to the user requirements, the management of the development organization may put additional requirements to ensure that the product is developed at a low cost and to ensure that the software can be maintained at low cost. If the management wants to modify customized software to make it a generic product later, additional requirement may be put such as portability.

Time

To deliver the product within the time frame without compromising on quality is another criterion for the success of a project. Many clients are ready to pay more money if necessary, but they do not like to compromise on time—after all time is money. But then, there is a problem. While giving the project proposal, the development time is estimated to be, say, 6 months. The client wants it in 3 months. To grab the order, in most cases, the manager will agree. Once the commitment is made to the client, it is the manager's responsibility to see that the project is completed within 3 months, then only the project is a success. Here, the perceptions differ—the manager may argue that even if it is delivered in 5 months, for him it is a success because it is

within his initial estimate. But the fact remains that the customer is the ultimate reference. More than the project team's perceptions, the perception of the customer is important.

Budget

Project costing is an extremely complex process. While giving a project proposal to the prospective customer, it may not be possible to foresee each item to be costed. A meticulous planning and foresight are required to do the project costing. As experience is the best teacher in project costing, the project manager must document all the factors that affect the project cost while executing each project. The process of cost estimation needs to be improved continuously. Another important aspect in estimation is the risk items. During project proposal preparation itself, the manager must analyze the likely risks and the corrective action to be taken and account for such costs as well. For instance, it is now common in some organizations for people to leave in the middle of the project [22].

6.8 White Box and Black Box Testing

Criteria	Black Box Testing	White Box Testing
Definition	Black Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is NOT known to the tester	White Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is known to the tester.
Levels Applicable To	Mainly applicable to higher levels of testing: Acceptance Testing System Testing	Mainly applicable to lower levels of testing: Unit Testing Integration Testing
Responsibility	Generally, independent Software Testers	Generally, Software Developers
Programming Knowledge	Not Required	Required
Implementation Knowledge	Not Required	Required
Basis for Test Cases	Requirement Specifications	Detail Design

Table 2: Black box vs White box testing (Adapted from [23])

Although white-box regression test prioritization has been well-studied, the more recently introduced black-box prioritization approaches have neither been compared against each other nor against more well-established white-box techniques. It presents a comprehensive experimental comparison of several test prioritization techniques, including well-established white-box strategies and more recently introduced black-box approaches. It has also been found that Combinatorial Interaction Testing and diversity-based techniques (Input Model Diversity and Input Test Set Diameter) perform best among the black-box approaches. Perhaps surprisingly, we found little difference between black-box and white-box performance (at most 4% fault detection rate difference). Also, it has been found that the overlap between black- and white-box faults to be high: the first 10% of the prioritized test suites already agree on at least 60% of the faults found. These are positive findings for practicing regression testers who may not have source code available, thereby making white-box techniques inapplicable [24].

Chapter 7 – Conclusion

7.1 Chapter Overview

The previous chapter discusses about the evaluation and testing process by using different methodologies on the proposed decentralized social application. This chapter will be mainly focused about concluding the proposed research with some highlighting achievements of the aim and objectives and will be discussing about the project life cycle along with the blockers and challenges that were faced during implementation of the system. More over the future enhancements also have been included in this chapter.

7.2 Achievements of Aims and Objectives

The major aim and objectives of this research, in the first place is that, to have a basic and strong understanding on the concepts such as blockchain, smart contract, decentralized app and how they all work together as a clique. Initially the author had put his effort on understanding every single concept theoretically and practically, by reading up a lot of research papers, blogs, and articles on the grey areas. He also happened to do a handful of tutorials which were available in the internet, in order to get familiar with the technologies. This technology stack has been entirely new for the author, and confusing at times since there were contradictory articles which were directing the author in various ways. Hence the author made sure to go with the trusted and proven resources such as the research papers and books.

Once making sure that the concepts were thorough, the author went ahead and looked upon the existing solutions which were out there with regards to a decentralized application with blockchain and smart contracts being involved. There were some of them which have been using by real time users currently, and there were other few areas in which people have tried to implement and have failed. So, the author wanted to pick one of those areas, which were failed to be implemented as a solution. Then he picked one as of, building a solution for the locals who’re travelling by train daily, assuming that it’ll be useful for them to know the statuses on any train which is available on an any given date. It will also allow the users to post real time comments as they travel in the train, so that the other passengers can utilize the real time services if they do have any cryptocurrency left in their account. Basically, there’ll be no third party involved in this to handle the transactions, but the passengers themselves. Hence it will be secured and less hassle.

Once identifying the core objectives after designing the diagram, the author starts to implement the design with the knowledge he gained from the tutorials and videos on the internet. There were so many blockers, since it was the first time that the author is trying to build a dapp based on blockchain and smart contracts. The major blockers were, the data that should be used for

this application, and how-to governance the data or maybe wrangle the data to use it as author needs in this perspective. Since there were dirty data or rather mis useful data, which needed to be cleansed before using it for the application. Moreover, the author himself, has collected some data from the passengers by recording the conversation with them. He has used that set data as well to bring in more clarity and meaningfulness. Another objective was to run this application in a larger scale, by bringing in the concept of Bigdata. That was the author's motive and end goal. In order to make that as a success, the author had to take certain measures such as the source of data, and the types of data that he'll receive from the sources, and the necessary data that should be wrangled in order to use it for the application. Once the cleansing is done, the author wanted to do a test run to see whether the core functionalities are working, plus whether the transactions have been handled properly. All sorts of testing approach were taken in to consider, which makes sure that this application wouldn't have flaws at any given time and will be able to handle any amount of load.

Another important objective was to document everything, as in the implementation steps, the deployment steps and the technologies and the versions that have been utilized etc. Once everything is documented in place, it will be easier for the other people who would read this thesis anytime in the future, or even enhance it and work on it. The implementation and the design details were discussed with the leads of the certain technologies and had a critical evaluation on what I need to change or what I need to enhance more.

7.3 Limitations of the research

This proposed decentralized application is unable to compare with existing solutions because some solutions haven't been published well. With that advantages and drawbacks and most of research papers didn't mention what were the technologies and the tools that they use to implement the algorithms or rather handling the cryptocurrency transaction, so it is hard to study the existing solutions properly. The technologies that are being used in this proposed system is vast and has a broader aspect. Hence, it was hard to narrow it down, or break it down into sub tasks before start working on it.

Another limitation which was faced by the author initially was, that what're the tools and technologies that should be selected in order to build this solution. Because, most of the technologies that are related to this solution, are completely new and haven't been tested or experienced by the author before this. Hence, he had to identify some of the experts in the domain or the grey area which he's lacking knowledge of, to understand the high-level pros and cons of picking a suitable technology as they're number of alternatives which can be used to do build this solution. Moreover, the other limitation was how the author could test all this among numerous users.

References

[1] "Towards secure e-voting using ethereum blockchain - IEEE Conference Publication", *Ieeexplore.ieee.org*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8355340/. [Accessed: 14- Sep- 2018].

[2] "Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage - IEEE Journals & Magazine", Ieeexplore.ieee.org, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8386868/. [Accessed: 14- Sep- 2018].

[3] G. Bowen, "Preparing a Qualitative Research-Based Dissertation: Lessons Learned", *NSUWorks*, 2019. [Online]. Available: https://nsuworks.nova.edu/tqr/vol10/iss2/2/. [Accessed: 24- Feb- 2019].

[4] *Elearning.ufl.udn.vn*, 2019. [Online]. Available: http://elearning.ufl.udn.vn/home/esp/pluginfile.php/3274/mod_resource/content/1/Judith%20Bell%20-%20Doing_Your_Research_Project.pdf. [Accessed: 24- Feb- 2019].

[5] *Elearning.ufl.udn.vn*, 2019. [Online]. Available: http://elearning.ufl.udn.vn/home/esp/pluginfile.php/3274/mod_resource/content/1/Judith%20Bell%20-%20Doing_Your_Research_Project.pdf. [Accessed: 24- Feb- 2019].

[6] *Knowledge4empowerment.files.wordpress.com*, 2019. [Online]. Available: https://knowledge4empowerment.files.wordpress.com/2011/06/denzin-lincoln_intro.pdf. [Accessed: 24- Feb- 2019].

[7] "Moore, D. S., & McCabe, G. P. (2005). Introduction to the Practice of Statistics (5th ed.). New York, NY W.H. Freeman & Company. - References - Scientific Research Publishing", *Scirp.org*, 2019. [Online]. Available: https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1385061. [Accessed: 24- Feb- 2019].

[8] K. Krippendorff and M. Bock, *The content analysis reader*. Thousand Oaks: Sage Publications, 2009.

[9] I. Sommerville, "Software Engineering", *Dl.acm.org*, 2019. [Online]. Available: https://dl.acm.org/citation.cfm?id=534403. [Accessed: 26- Feb- 2019].

[10] P. Hubbard, "SAGE Journals: Your gateway to world-class journal research", *Journals.sagepub.com*, 2019. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1080/0042098966745. [Accessed: 26- Feb- 2019].

[11] C. Dannen, "Introducing Ethereum and Solidity | SpringerLink", *Link.springer.com*, 2019. [Online]. Available: https://link.springer.com/book/10.1007%2F978-1-4842-2535-6. [Accessed: 27- Feb- 2019].

[12] F. Olleros and M. Zhegu, *Research handbook on digital transformations*.

[13] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, *BlockChain Technology: Beyond Bitcoin*, 2nd ed. California: Applied Innovation Review, 2016, pp. https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf.

[14] M. Raskin, "THE LAW AND LEGALITY OF SMART CONTRACTS", *Georgetownlawtechreview.org*, 2019. [Online]. Available: https://georgetownlawtechreview.org/wp-content/uploads/2017/04/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf. [Accessed: 27- Feb- 2019].

[15] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things - IEEE Journals & Magazine", *Ieeexplore.ieee.org*, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7467408/. [Accessed: 27- Feb- 2019].

[16] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview - IEEE Conference Publication", Ieeexplore.ieee.org, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8345547. [Accessed: 28- Feb- 2019].

[17] V. Buterin, "Ethereum White Paper", Blockchainlab.com. [Online]. Available: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. [Accessed: 28- Feb- 2019].

[18] "How Ethereum Works - CoinDesk", CoinDesk, 2019. [Online]. Available: https://www.coindesk.com/information/how-ethereum-works. [Accessed: 28- Feb- 2019].

[19] M. Bollapragada, "Agile vs Iterative vs Waterfall models", Slideshare.net, 2019. [Online]. Available: https://www.slideshare.net/MarrajuBollapRagada/agile-vs-iterativevswaterfall. [Accessed: 22- Apr- 2019].

[20] P. Hampton, "Intro to Blockchain With Ethereum, Web3j and Spring Boot: Smart Contracts | trade bitcoins, altcoins 101,trade cryptocurrencies, trade altcoins, information, cryptocurrency 101,dapp,bitcoin101,bitcoin,storj,sia,articles,markets,dao,counterparty,altcoins,exchange,purchase bitcoins,exchanges,news,101,mining bitcoins, buy bitcoins, sell bitcoins, mining coins,ethereum,bitcoin excahnge,tickers - Coin Spectator", Coinspectator.com, 2019. [Online]. Available: https://coinspectator.com/news/673174/intro-to-blockchain-with-ethereum-web3j-and-spring-boot-smart-contracts. [Accessed: 22- Apr- 2019].

[21] "Software Design Methodology", Userpages.umbc.edu, 2019. [Online]. Available: https://userpages.umbc.edu/~khoo/survey1.html. [Accessed: 22- Apr- 2019].

[22] "Criteria for the Success of a Software Project in Testing Tools Tutorial pdf - Criteria for the Success of a Software Project in Testing Tools (14402) | Wisdom Jobs", Wisdom Jobs, 2019. [Online]. Available: https://www.wisdomjobs.com/e-university/testing-tools-tutorial-239/criteria-for-the-success-of-a-software-project-14402.html. [Accessed: 22- Apr- 2019].

[23] "Differences Between Black Box Testing and White Box Testing - Software Testing Fundamentals", Software Testing Fundamentals, 2019. [Online]. Available: http://softwaretestingfundamentals.com/differences-between-black-box-testing-and-white-box-testing/. [Accessed: 22- Apr- 2019].

[24] C. Henard, M. Papadakis, M. Harman, Y. Jia and Y. Le Traon, "Comparing white-box and black-box test prioritization", Proceedings of the 38th International Conference on Software Engineering - ICSE '16, 2016. Available: 10.1145/2884781.2884791 [Accessed 22 April 2019].

[25] Codementor.io. (2019). Developing for Ethereum: Getting Started with Ganache | Codementor. [online] Available at: https://www.codementor.io/swader/developing-for-ethereum-getting-started-with-ganache-l6abwh62j [Accessed 28 Apr. 2019].

[26] (2019). Getting started with Ganache: your personal blockchain for Ethereum development — Steemit. [online] Steemit.com. Available at: https://steemit.com/utopian-io/@icaro/getting-started-with-ganache-your-personal-blockchain-for-ethereum-development [Accessed 28 Apr. 2019].

[27] Medium. (2019). What is MetaMask? Really… What is it?. [online] Available at: https://medium.com/@seanschoi/what-is-metamask-really-what-is-it-7bc1bf48c75 [Accessed 28 Apr. 2019].

[28] Bitfalls. (2019). What is MetaMask and How to Send and Receive Ether with it? - Bitfalls. [online] Available at: https://bitfalls.com/2018/02/16/metamask-send-receive-ether/ [Accessed 28 Apr. 2019].

[29] Solidity.readthedocs.io. (2019). Introduction to Smart Contracts — Solidity 0.5.6 documentation. [online] Available at: https://solidity.readthedocs.io/en/v0.5.6/introduction-to-smart-contracts.html [Accessed 28 Apr. 2019].

[30] Blockonomi. (2019). What is Solidity? Our Guide to the Language of Ethereum Smart Contracts. [online] Available at: https://blockonomi.com/solidity-guide/ [Accessed 28 Apr. 2019].

[31] Theethereum.wiki. (2019). Remix - The Ethereum Wiki. [online] Available at: https://theethereum.wiki/w/index.php/Remix [Accessed 28 Apr. 2019].