Department of Computer Science & Engineering

Project Report

Own Token Sale

Course Title: Software Development IV

Course No: CSE 400

Submitted by

Sadia Islam Asha (16172103034)
Tanvir Ahamed Anik (16172103004)
Afra Anjuman Anti (16172103019)
Md. Zahidul Islam (16172103451)
Md. Kamruzzaman (16172103038)

Program: BSc. Engg in CSE , Intake: 35, Section: 01

Submitted to

Moniruz Zaman
Lecturer, Department of CSE

Bangladesh University of Business and Technology (BUBT)

Date of submission: 23.08.2020

Abstract

Initial Coin Offering (ICO) is a process similar to crowd funding, in which companies raise funds from investors, who in return receive tokens or digital assets. With conventional methods of crowd funding, the level of transparency depends on a centralized platform used in campaigns. With the emergence of peer-to-peer digital currency systems, also known as cryptocurrencies, it became possible to implement crowd funding campaign sin a fully transparent way for investors. Public sales of blockchain digital assets are known as crowd sales which are implemented using blockchain smart contracts. The paper presents a solution for automating ICO processes implemented using the Ethereum blockchain and explain the basics of crowd sale token sale flow. Next, we analyze features vital for transparent ICO execution as well as the benefits and costs of running an ICO on cryptocurrency application platforms.

Acknowledgement

First of all we would like to thank the Almighty Allah who is always the one giving us confidence and patience to do this work. Without His grace this thesis couldn't become a reality.

We would like to express our sincere gratitude to our supervisor Moniruz Zaman, Lecturer without whom this project work would not exist in its present form. We are feeling oblige in taking the opportunity to sincerely to all our team members because without their contribution we couldn't think to take this project become reality. Every team members did really hard work for this project so we are really thankful to all of our members.

A special thanks to our family. Words can’t express how grateful we are to our parents because without them we couldn't see this beautiful world and whose we are greatly indebted for us bought up with love and encouragement to this stage.

Contents

Chapter 1

Introduction

1.1 Introduction

Currently tokens are a well-known concept that is used to represent something unique. One of the most complex challenges is to gain full understanding of them. The first wave of blockchain projects have mostly been pioneering testing grounds for a new technology which now is widely seen by many as a disruptive force for cross-domain innovation. With the emergence of blockchain-based projects for every imaginable domain and a growing ambitious vision on what the technology can truly achieve, there has been a corresponding increase in the complexity of token design. Adding to this the constant resort to ICOs and Token Sales as funding schemes for many of these projects, and evidence has risen on the widening scope of misunderstandings and the lack of information surrounding tokens and the true value of the claim they represent. These are symptoms perceived by many as growth pains in a technology still constantly facing new challenges.

The blockchain technology has evolved since the Bitcoin invention and today there are various blockchain platforms that can store and execute code by using the so-called smart contracts on thousands of nodes. These platforms, e.g. Ethereum, have allowed people to create their own cryptocurrencies, tokens and new forms of digital assets. Such programmable blockchains have resulted in the emergence of a novel concept known as the Initial Coin Offering (ICO).

This paper fills in this gap and presents details of a token implementation based on Ethereum as well as an extensive analysis of benefits and execution costs of token features implemented using Ethereum's smart contracts.

1.2 Existing Theory

We highlight the following contributions:

•Design and implementation of an ICO (token) platform based on Ethereum,

•Performance evaluation of the corresponding ICO processes running on Ethereum, and

•An analysis of features commonly implemented in an ICO.

1.3 Scope of the Research

Cryptocurrencies and blockchain are a monstrous topic. There are several hundreds of cryptocurrencies and the applications of blockchain technology are also numerous. To make this research a useful and focused one, we have to narrow it down. To do this, the research attaches to multiple connecting factors, defining its scope.

Firstly, the research is limited to cryptocurrencies and blockchain. This means that other types of assets than cryptocurrencies, such as tokens or crypto securities, are not within the scope of this research. We will explain how these assets differ from cryptocurrencies further on. We will also not elaborate on derivatives of cryptocurrencies, which are essentially investment instruments.

Blockchain will be scrutinized to the extent cryptocurrencies run on this technology. Therefore, blockchain technology will not be looked at outside of the context of cryptocurrencies, such as it being used as a technique to eliminate intermediaries in the financial, public or other sector. This would lead to far and exceeds the scope of this research. Secondly, the research relates to the legal context of cryptocurrencies and blockchain.

The focus is, hence, a legal one. This means that we will not elaborate on all the technical aspects – and there are many – relating to cryptocurrencies and blockchain. We will only touch upon those to the extent necessary to understand the legal context. We will also not take an economic, criminological or any other approach than a legal one.

1.4 Objectives

Cryptocurrencies and blockchain have become hot topics in the last couple of years. Whilst the two are often referred to in the same sentence and are clearly linked to each other, one should never mistake one for the other. Blockchain is a type of distributed ledger technology that forms the backbone of the crypto-market.

- It is the technology behind the large variety of cryptocurrencies currently in circulation.
- Its scope and field of application are, however, not limited thereto.
- As set out above, blockchain can be applied in various sectors and can have a wide array of applications.

It is important to draw a clear line between these applications and cryptocurrencies, which are but one specific application of blockchain technology.

1.5 Organization of Project Report

The project work is organized as follows.

Chapter 1 the introduction of the project of own token sale.

Chapter 2 highlights the existing system.

Chapter 3 describes the concepts of token economy, token types, and the case for using tokens.

Chapter 4 contains the proposed architecture of the own token sale along with a detailed walk through of the overall.

Chapter 5 includes the details of the tests and evaluations that were performed to evaluate our proposed architecture.

Finally, Chapter 6 contains the overall conclusion of our project work.

1.6 Conclusion

This chapter includes a comprehensive overview of the problem that we specifically target, the objectives of our project work along with the motivation of the output of the project work. This section also illustrates the overall steps on which we carried out our project work.

Chapter 2
Existing System

2.1 Introduction

Blockchain is a specialization of a distributed ledger technology (DLT). DLTs enable the maintenance of a global, append-only data structure by a set of mutually untrusted parties in a distributed environment. Blockchain technology gives advantages such as transaction security,

process identification, process automation and payment speed. A blockchain account can provide functions other than making payments, for example in decentralized applications or smart contracts. In this case, the units or coins are sometimes referred to as crypto tokens.

Cryptography has several important roles in a blockchain platform: user identification with PKI infrastructure, digital signing and ability to achieve global consensus with hash functions combined with consensus mechanisms. Bitcoin and Ethereum use Elliptic Curve Digital Signature Algorithm (ECDSA) [16] to create private keys and derived corresponding public keys, which are, when hashed, also wallet public addresses. Digital signatures are one of the fundamental technologies for identity verification in cryptocurrency platforms.
Cryptographic hash functions are a special class of hash functions which are used for reaching global consensus in a blockchain platform. They are deterministic, they will always generate the same random bytes for the same input, and a small change in the input should result in a completely different hash. These features make hash functions ideal for implementing distributed consensus mechanism.

2.2 Existing System

In this work, each role is based on a distinct purpose and exhibits different features, where by tokens can exhibit more than one role.

- Though this provides flexibility by compounding different utility factors.
- Firstly, we interpret utility as a more volatile dimension. We perceive utility instead as a spectrum which is hardly pre-classifiable due to the high variability in which it can emerge in a specific token.
- A token exists either because it uniquely represents an asset.
- Following an existing classification (Mougayar 2017), tokens may bestow a right to its holder (Right), represent a unit of value exchange in an internal system.
- Depict a fee for pay-per-use or access purposes to a platform (Toll).

2.3 Existing Literature

There are various IEEE papers which gives idea about the Recommender Systems. For our system we have referred papers as follows:

2.3.1

Bitcoin [1], the world's first cryptocurrency, was designed and implemented in 2009 by an unknown author, known only under the pseudonym Satoshi Nakamoto. He designed a decentralized peer-to-peer cash system which solves the double spending problem and allows online payments to be sent directly from one entity to another without central financial intermediaries. For solving the double spending problem, a peer-to-peer distributed timestamp server is used to generate computational proof of the chronological order of transactions, using cryptographic hash functions.

2.3.2

Initial Crypto asset Offering (ICO), also often called Initial Coin Offering or Initial Token Offering (ITO) is a new means of fundraising through blockchain technology, which allows startups to raise large amounts of funds from the crowd in an unprecedented speed. Key information about ICOs collected by these websites are categorized, and key factors that differentiate the evaluation mechanisms employed by these evaluation websites are identified. In this paper we present the first findings of an analysis of a set of 28 ICO evaluation websites, aiming at revealing the state of the practice in terms of ICO evaluation.

2.3.3

Despite this, in view of the absence of regulatory and legal regulation, basic concepts, methods of evaluation, management and optimization of crypto-economics processes have not yet been formulated. The present study is devoted to the pricing of ICO as a source of financing for the activities of enterprises that are used practically in all sectors of the economy. This current trend has taken shape and has taken its place in the current economic environment.

2.3.4

Digital assets (tokens) are listed and sold at online platforms during events called crowd sales, which are similar to crowd funding processes, but they are usually decentralized and transparent. Blockchain and cryptocurrencies represent a disruptive technology which has reached its peak in 2018. In the first two quarters of 2018, 271 ICOs were noted with more than 7billions of dollars collected.

2.3.5

The author compared the gathered data in order to be able to define the quality of the evaluation websites regarding completeness and clarity of the shown information, finding several differences in rating parameters and ICO distribution. The evaluation websites of ICO (Initial coin offering) a way to raise funds for creating a new coin, app, or service launches, represent the main source where investors can find interesting information about their investments on one or more ICOs.

2.4 Conclusion

This chapter includes a comprehensive overview of the existing systems and the problem that we specifically target to solve.

Chapter 3

Concepts of Tokens

3.1 Token Economy

An increasing number of projects based on blockchain platforms is emerging almost every day, and they appear to be tokenizing everything. Not all ICOs are equal, and not all tokens are equal. There are three main types of tokens: cryptocurrency tokens, security tokens, and utility tokens.

Cryptocurrency tokens, also known as consensus or payment tokens, are what is known as cryptocurrencies - digital assets which are in the core of blockchain platforms, like Ether in

Ethereum or Bitcoin in Bitcoin. A consensus token is an incentive given as a reward for validating transactions in the cryptocurrency platform.

Security tokens, also known as equity tokens, represent ownership shares of a company or DAO platform. DAO is a decentralized autonomous organization, governed by people or companies which vote using smart contracts or a similar concept.

Utility tokens, also known as an application or user coins, provide a user with future access to a product or service or are needed for using the product or services. If a token is legally classified as a security, token issuers are legally responsible to their investors. Developers of a platform which use utility tokens are not so strictly legally responsible to their investors and are subject to milder laws than those which use security tokens.

3.2 Classifying Tokens

This step extends the task of perceiving the purpose of a specific token. Many classifications have been proposed on how to differentiate tokens based on a specific property. While some of them are more widely used than others, there is still a lack of agreement on whether and how these can be arranged.

1. One such example is the general distinction between cryptocurrencies and tokens. Although both domain literature and online market trackers usually tend to agree on the distinction between coins or cryptocurrencies -which are native to a blockchain -and blockchain tokens -which are created on top of a blockchain, depend on it and governed by smart contracts, this differentiation is based on the technical layer in which the asset is built on, and does not pertain to the role which the asset takes.
2. Other authors interpret the difference between both cryptocurrencies and tokens by differentiating, respectively, between those which have the ambition to become de facto digital currencies and those whose purpose is tied to its platform's business model and long-term value.
3. Following this differentiation approach, a third classification usually arises in the form of equity tokens, or tokenised securities).

4. In this sense, the distinction is not (solely) based on the technical layer anymore, but rather on the purpose of the asset, or the function it takes form of in the eyes of its holder.
5. An additional popular token classification is based on its functional ability. In this realm, usage tokens are contrasted to work tokens, and sometimes even accompanied by hybrid tokens which represent a mixture of both.

3.3 The Case of Tokens

The purpose of issuing tokens tends to be justified by its role in the following dimensions:

•**Currency:** by acting as transmission of value, unit of account and store of wealth.

•**Validation Incentive:** by ensuring distribution consensus and data consistency.

•**Usage Incentive:** by allowing access or promoting platform usage.

•**Tool for Accelerating Network Effects:** by incentivizing early adoption.

•**Tool for Governance:** by preventing spamming or providing rights to participate in the platform's development.

•**Representation of Asset Ownership:** by encapsulating asset-backed or asset-based property rights.

•**Profit-Sharing:** by conferring its owner the claim to dividends or equivalents.

•**Funding Instrument:** by using the proceeds of a token sale to fund the development team or the community.

All these dimensions -except perhaps for the funding one -address the need to tie an adequate value container to the network's growth and, sometimes, to its internal incentive system. Without this value container, goes this logic, and the business model would likely either not function as intended or not even work at all.

Chapter 4
Proposed Method

4.1 Introduction

ICO is a process that enables companies and startups to raise funds from investors, who in return receive tokens or some other kind of digital assets. ICO owners use collected funds to develop their product(s) which will then provide additional features to investors and their accounts, e.g., investors can exchange their tokens for free company services or get discounts. Another way of integrating investors into a future product is by making them product shareholders. In such scenario, digital assets or tokens represent proof of ownership of product shares.

4.2 Requirement Analysis

An ICO is often used for raising funds because it simplifies a rigorous capital-raising process. ICOs promise quick liquidity, immutable contract guarantees, and democratic access to investment capital. A digital asset which is used in an ICO is often in the form of a token issued on a blockchain platform.

In particular, the following mechanisms and features are implemented and analyzed in this paper:

•**Mintable token:** a token that does not have an initial supply, but is rather minted when an investor buys tokens (more details are given in following sections);

•**KYC** is needed to ensure that only one physical person is represented by one account, to ensure a person's identity and prevent money laundering; in particular–Whitelisting: only people and their accounts which are in a whitelist can make token purchases–Individual capping: every account has an upper limit of monetary units which he/she can invest

•**Timeframe:** crowd sale is defined by time boundaries, and token purchases can be made only in the period between its opening and closing time;

•**Genesis allocation:** an initial allocation of tokens for the ecosystem (team, advisors, and developers);

•**Private investment:** a mechanism enabling private investors to buy tokens without exposing their identities;

•**Rate change:** a rate decreases linearly from public sale time to crowd sale ending time to encourage investors to buy tokens as soon as possible and to reach the goal at an early stage of the crowd sale;

•**Token refunding:** a mechanism to return a token to an investor who accidentally tried to invest some other token instead of cryptocurrency monetary units;

•**Refunding:** a mechanism to return monetary units to investors if a crowd sale has not been successful and its soft cap has not been reached;

•**Ecosystem time lock:** a mechanism for the ecosystem to ensure that investors cannot withdraw all their allocated tokens immediately after crowd sale has ended and sell it on an exchange market;

•**Bonus for high-level purchase:** bonus rate for the investor who makes a high-level purchase;

4.3 System Design

System design is the process of designing the elements of a system such as the architecture, modules and components, the different interfaces of those components and the data that goes through that system. The designing elements of our system are given below-

4.3.1 Flow Chart

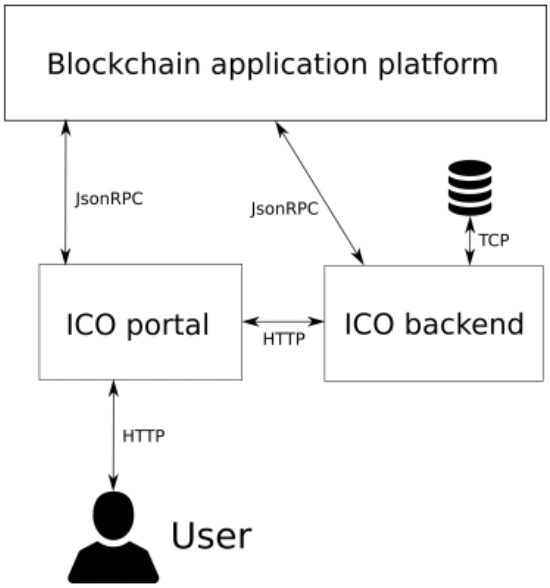

Fig: The system architecture of a crowd sale platform

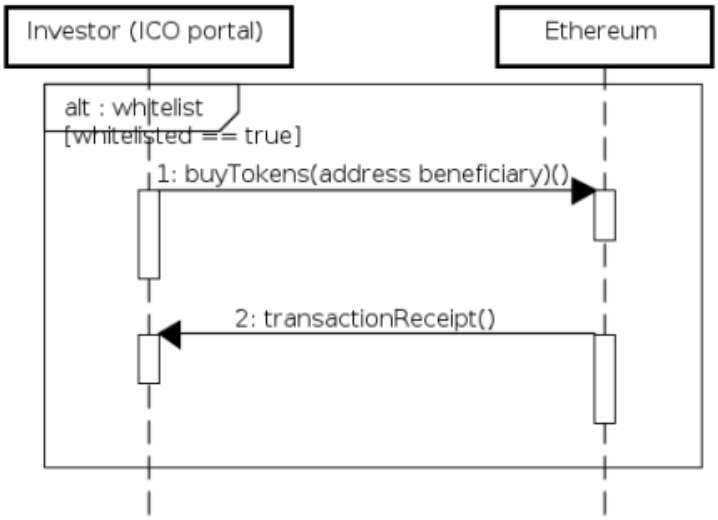

Fig: Token Purchase

4.4 Implementation

The eleven token parameters on the first column describe the token along its attributes:

•**Class:** a widely used distinction, thus distinguishing digital money (Cryptocurrencies), from digital shares with entitlement to profit-sharing or dividends (Tokenized Security) and from the remaining crypto-assets (Utility Tokens). This is a key distinction which lends a comfortable categorization to tokens with attached utility, thereby differentiating them from securities under strict legal supervision as well as from digital money such as Bitcoin, which as pure means of transaction has different ambitions.

•**Purpose:** a token exists either because it uniquely represents an asset (Asset-Backed), it confers to its holder an access permission just like an access card does (Usage Token) or it is used as value container to reward a certain behavior (Work Token).

•**Role:** following an existing classification, tokens may bestow a right to its holder (Right), represent a unit of value exchange in an internal system (Value Exchange), depict a fee for pay-per-use or access purposes to a platform (Toll), embody a tool to enrich user experience and reward user behavior, constitute a de facto payment method (Currency) or embody the right to confer profit-sharing to the token holder (Earnings).

•**Representation:** following an existing classification, tokens may represent pure digital assets like

voting rights or digital identities (Digital), be bound to physical objects as in smart property or smart objects (Physical), be tied to virtual reality objects (Virtual) or represent legal rights granted by law or agreed between parties (Legal).

•**Supply:** Describes whether a token supply is fixed and distributed on a one-time basis (Fixed) or behaves according to a specific schedule (Schedule-based).

•**Incentive System:** Tokens exert influence over the network and its holder through incentives which may be to Enter, Use or Stay Long-Term in a Platform.

•**Transactions:** Tokens which can be spent in a platform are considered Spendable, whereas the remaining are Non-Spendable.

•**Ownership:** In most cases tokens' ownership may change hands (Tradable), though there are cases where this is not possible (Non-Tradable) (Yadav 2017).

•**Chain**: The chain on which the protocol is based also affects token design. These can be new chains on new code, new chains on forked code, forked chains on forked code or -in the case of application-layer tokens –cases where the tokens are issued on top of a protocol.

Chapter 5

Experimental Results

5.1 Introduction

The proposed crowd sale platform is implemented using the Ethereum platform. The Ethereum platform was selected for implementation of an ERC20 token and crowd sale smart. Token purchase contract because it is currently the most stable platform for developing smart contracts and decentralized applications. Solidity is the programming language for developing smart contracts on Ethereum.

The basic crowd sale token sale flow consists of several steps. In the pre-validation phase, in which is checked whether the user has the rights to buy tokens. These checks can include KYC compliance, whether the user has necessary funds for a purchase, has the crowd sale ended, etc. Next phases are related to calculating the number of tokens, processing purchase, and updating the purchased state. The last phase is forwarding tokens to the user and post-validation of purchase.

Chapter 6

Conclusion

6.1 Conclusions

Cryptocurrencies are a new kind of digital assets and their expansion cannot be ignored. Despite the skepticism and controversy, they represent an innovative technical break through which is based on sound principles. Cryptocurrency systems offer a distributed, transparent ledger of transactions that can-not be updated and changed, and thus can be applied in many different fields not necessarily related to financial services. Smart contracts on the Ethereum blockchain offer much more than simple transactions and multi signature wallets; they offer a flexibility of a Turing-complete language for development of smart contracts and decentralized applications.

6.2 Future Work

We have tried our best to complete our project but there are still some limitations. We will surely fix them in future. The future of cryptocurrencies greatly depends on new solutions for scalability problems, because Proof-of-Work cryptocurrencies like Bitcoin or Ethereum can process only up to 15 transactions per second. Practical solutions to scalability issues and development of user-friendly interfaces to cryptocurrency wallets will determine whether smart contracts are accepted among the user.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,”https://www.bitcoin.org, p. 9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. F. Hartmann, X. Wang and M. I. Lunesu, "Evaluation of initial cryptoasset offerings: the state of the practice," 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, 2018, pp. 33-39, doi: 10.1109/IWBOSE.2018.8327569.
3. D. S. Demidenko, E. D. Malevskaia-Malevich and Y. A. Dubolazova, "ISO as a real source of funding. Pricing issues," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 622-625, doi: 10.1109/ICOIN.2018.8343193.

4. D.Floyd,“$6.3billion:2018ICOfundinghaspassed2017’stotal,”https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/, 2018, [Online;accessed 10-June-2018]
5. M. I. Lunesu and O. Desogus, "ICO Evaluation Websites Analysis," 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), London, ON, Canada, 2020, pp. 48-56, doi: 10.1109/IWBOSE50093.2020.9050259.